DoD 5015.2-STD

DRAFT

DESIGN CRITERIA STANDARD
FOR
ELECTRONIC RECORDS
MANAGEMENT
SOFTWARE APPLICATIONS

ASD NII/DOD CHIEF INFORMATION OFFICER

FOREWORD GOES HERE

TABLE OF CONTENTS

TABLE OF CONTENTS (continued)

Page

TABLES

APPENDICES

(This page intentionally left blank.)

REFERENCES

(a) DoD Directive 5015.2, "Department of Defense Records Management Program," March 6, 2000

(b) DoD 5015.2-STD, “Design Criteria Standards for Electronic Records Management Software Applications,” June 19, 2002 (hereby canceled)

(c) Department of Defense Discovery Metadata Specification (DDMS), Version 1.3, 29 July 2005

(d) Executive Order 12958, “Classified National Security Information,” as amended by Executive Order 13292, "Further Amendments to Executive Order 12958," March 28, 2003

(e) National Archives and Records Administration, "Records Management Handbook — Disposition of Federal Records," 1996

(f) Title 36, Code of Federal Regulations, Part 1236.14, "Definitions," current edition

(g) Title 36, Code of Federal Regulations, Part 1234.2, "Definitions," current edition

(h) National Archives and Records Administration, "Managing Electronic Records Instructional Guide," "Appendix F, Glossary," 1990

(i) Title 36, Code of Federal Regulations, Part 1228.58, "Destruction of Temporary Records," current edition

(j) Title 36, Code of Federal Regulations, Part 1228.60, "Donation of Temporary Records," current edition

(k) Section 3301 of title 44, United States Code, "Definition of Records"

(l) Title 36, Code of Federal Regulations, Part 1220.14, "General Definitions," current edition

(m) Section 3511 of title 44, United States Code, "Establishment and Operation of Government Information Locator Service"

(n) Federal Information Processing Standard Publication 192, "Application Profile for the Government Information Locator Service," December 7, 1994

(o) Section 2901 of title 44, United States Code, "Definitions"

(p) Section 2902 of title 44, United States Code, "Objectives of Records Management"

(q) Section 3103 of title 44, United States Code, "Transfer of Records to Records Centers”

(r) Title 36, Code of Federal Regulations, Part 1222.10, "Authority," current edition

(s) ISO 8601, "Data elements and interchange formats – Information interchange – Representation of dates and times," 2004

(t) Title 36, Code of Federal Regulations, Part 1194.21, "Software Applications and Operating Systems," current edition

(u) Title 36, Code of Federal Regulations, Part 1194.31, "Functional Performance Criteria," current edition

(v) Title 36, Code of Federal Regulations, Part 1194.22, "Web-based Intranet and Internet Information and Applications," current edition

(w) Section 794d of title 29, United States Code, "Electronic and Information Technology"

(x) Section 3303 of title 44, United States Code, "Lists and Schedules of Records"

(y) Title 36, Code of Federal Regulations, Part 1222.50, "Records Maintenance and Storage," current edition

(z) Records Management Task Force, "Functional Baseline Requirements and Data Elements for Records Management Application Software," August 28, 1995

(aa) Title 36, Code of Federal Regulations, Part 1228.24, "Formulation of Agency Records Schedules," current edition

(ab) Title 36, Code of Federal Regulations, Part 1236.20, "Vital Records Program Objectives," current edition

(ac) Title 36, Code of Federal Regulations, Part 1234.22, "Creation and Use of Text Documents," current edition

(ad) Director of Central Intelligence Directive (DCID) 6/6, "Security Control on the Dissemination of Intelligence Information," July 11, 2001

(ae) DoD Directive 5210.83, "Department of Defense Unclassified Controlled Nuclear Information (DoD UNCI)," November 15, 1991

(af) DoD 5400.7-R, "DoD Freedom of Information Act Program Regulation" September 1998

(ag) DoD Directive 5230.24, "Distribution Statements on Technical Documents," March 18, 1987

(ah) DoD 5200.1-R, "Information Security Program Regulation," January 14, 1997

(ai) Title 36, Code of Federal Regulations, Part 1234.32, "Retention and Disposition of Electronic Records," current edition

(aj) Title 36, Code of Federal Regulations, Part 1222.32, "General Requirements," current edition

(ak) Title 36, Code of Federal Regulations, Part 1234.24, "Standards for Managing Electronic Mail Records," current edition

(al) Section 3105 of title 44, United States Code, "Safeguards"

(am) Title 36, Code of Federal Regulations, Part 1234.28, "Security of Electronic Records," current edition

(an) Section 2909 of title 44, United States Code, "Retention of Records"

(ao) Title 36, Code of Federal Regulations, Part 1228.54, "Temporary Extension of Retention Periods," current edition

(ap) Title 36, Code of Federal Regulations, Part 1228.270, "Electronic Records," current edition

(aq) Title 36, Code of Federal Regulations, Part 1234.34, "Destruction of Electronic Records," current edition

(ar) Executive Order 12968, "Access to Classified Information," August 4, 1995

(as) Title 36, Code of Federal Regulations, Part 1234.30, "Selection and Maintenance of Electronic Records Storage Media," current edition

(at) Title 32, Code of Federal Regulations, Part 2001, "Classified National Security Information," current edition

(au) 5 U.S.C. § 552a, "The Privacy Act of 1974 As Amended," 2004

(av) DoD 5400.11-R, "Department of Defense Privacy Program," August 1983

(aw) Universal Description, Discovery and Integration v3.0.2 (UDDI), February 2005

(ax) DoD Information Management (IM) Strategic Plan, Version 2.0, October 1, 1999

(ay) C4ISR Architecture Framework, Version 2.0, December 18, 1997

(az) Global Information Grid Architecture, current version

(ba) Global Information Grid Capstone Requirements Document, JROCM 134-01, August 30, 2001
(bb) DoD Directive 4630.5, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," May 4, 2004
(bc) DoD Chief Information Officer Memorandum “DoD Net-Centric Data Strategy,” May 9, 2003
(bd) DoD Directive 8320.2, “Data Sharing in a Net-Centric Department of Defense,” December 2, 2004

(This page intentionally left blank.)

DL1.1. DEFINITIONS

DL1.1.1. Access. The ability or opportunity to gain knowledge of stored information.

DL1.1.2. Access Control. The term access control has the following meanings:

DL1.1.2.1. A service feature or technique used to permit or deny use of the components of a communication system.

DL1.1.2.2. A technique used to define or restrict the rights of individuals or application programs to obtain data from, or place data onto, a storage device.

DL1.1.2.3. The definition or restriction of the rights of individuals or application programs to obtain data from, or place data into, a storage device. There are several types of access control; for example Role Based Access Control, Mandatory Access Control, and Discretionary Access Control.

DL1.1.2.4. The process of limiting access to the resources of an AIS to authorized users, programs, processes, or other systems.

DL1.1.2.5. That function performed by the resource controller that allocates system resources to satisfy user requests.

DL1.1.3. Accession. To transfer physical and legal custody of documentary materials to an archival institution.

DL1.1.4. Addressee. The name of the organization to which or individual to whom a record is addressed.

DL1.1.5. Application Administrators. Individuals who are responsible for setting up the RMA infrastructure.

DL1.1.6. Attachment. A record, object, or document associated with another document or record and filed in the RMA or transmitted as part of the other document or record.

DL1.1.7. Attribute. A name-value pair associated with an element. An attribute is not a standalone element, but data detail contained within an element (see DDMS , reference (c)).

DL1.1.8. Audit Trail. An electronic means of tracking interactions with records within an electronic system so that any access to the record within the electronic system can be documented as it occurs or afterward. May be used to identify unauthorized actions in relation to the records, e.g., modification, deletion, or addition.

DL1.1.9. Authenticity. A condition that proves that a record is genuine based on its mode (i.e., method by which a record is communicated over space or time), form (i.e., format or media that a record has upon receipt), state of transmission (i.e., the primitiveness, completeness, and effectiveness of a record when it is initially set aside after being made or received), and manner of preservation and custody.

DL1.1.10. Authorized Individual. A Records Manager or other person specifically designated by the Records Manager as responsible for managing various aspects of an organization's records.

DL1.1.11. Author, Originator, or Creator. The author of a document is the person, office or designated position responsible for its creation or issuance. The author, originator, or creator is usually indicated on the letterhead or by signature. For RMA purposes, the author, originator, or creator may be designated as a person, official title, office symbol, or code.

DL1.1.12. Auto-filing. The ability of an RMA to automatically file records without user intervention.

DL1.1.13. Backward Compatible. The ability of a software program or piece of hardware to read files in previous versions of the software or hardware.

DL1.1.14. Biometrics. Measurable physical characteristics or personal behavioral traits used to recognize the identity or verify the claimed identity of an individual..

DL1.1.15. Boolean Operators. The operators of Boolean algebra may be represented in various ways. Often they are simply written as AND, OR and NOT. While any number of logical ANDs (or any number of logical ORs) may be chained together without ambiguity, the combination of ANDs and ORs and NOTs can lead to ambiguous cases. In such cases, parentheses may be used to clarify the order of operations. As always, the operations within the innermost set of parens is performed first, followed by the next set out, etc., until all operations within parens have been completed. Then any operations outside the parentheses are performed.

DL1.1.16. Bulk Load. Automatically importing data.

DL1.1.17. Business Rules. Business rules describe the operations, definitions and constraints that apply to an organization in achieving its goals. For example a business rule might state that no credit check is to be performed on return customers. Others could define a tenant in terms of solvency or list preferred suppliers and supply schedules. These rules are then used to help the organization to better achieve goals, communicate among principals and agents, communicate between the organization and interested third parties, demonstrate fulfillment of legal obligations, operate more efficiently, automate operations, perform analysis on current practices, etc.

DL1.1.18. Cascading Style Sheets. Cascading Style Sheets (CSS) is a stylesheet language used to describe the presentation of a document written in a markup language. Its most common application is to style web pages written in HTML and XHTML, but the language can be applied to any application of XML, including SVG and XUL. The CSS specifications are maintained by the World Wide Web Consortium (W3C).

DL1.1.19. Classified Information. Information that has been determined pursuant to EO 12958, as amended by EO 13292 (reference (d)) or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

DL1.1.20. Classification Markings. Identifications or markings that leave no doubt about the classified status of the information, the level of protection required and the duration of the classification. Such markings include: Overall Markings, Portion Markings, Classified by line, Reason line, Derived from line, and Declassify on line (see reference (d)).

DL1.1.21. Common Access Cards (CAC). Cards that feature bar-coding, a magnetic strip, and an embedded integrated circuit chip used for access to buildings, to computer systems, etc.

DL1.1.22. Compression. A process, using special software, that reduces the file size of a given electronic file.

DL1.1.23. Copy. In electronic records, the action or result of reading data from a source (RMA's repository), leaving the source data unchanged, and writing the same data elsewhere on a medium that may differ from the source (user workspace or other device) (see RM Handbook, reference (e)).

DL1.1.24. Create. In electronic records, the action or result of filing a new record and its associated metadata.

DL1.1.25. Creator. See DL1.1.11.

DL1.1.26. Cutoff. To cut off records in a file means to break, or end, them at regular intervals to permit their disposal or transfer in complete blocks and, for correspondence files, to permit the establishment of new files. Cutoffs are needed before disposition instructions can be applied because retention periods usually begin with the cutoff, not with the creation or receipt, of the records. In other words, the retention period normally does not start until the records have been cut off. Cutoffs involve ending input to old files and starting input to new ones at regular intervals (see reference (e)). Cutoff is sometimes abbreviated as COFF and is also called file cutoff or file break.

DL1.1.26.1. For records with retention periods of less than 1 year. Cut off at an interval equal to the retention period. For example, if a record series has a 1-month retention period, cut the file off at the end of each month and then apply the retention period (that is, hold the file 1 more month before destroying it).

DL1.1.26.2. For records with retention periods of 1 year or more. Cut off at the end of each fiscal (or calendar) year. For example, if the disposition instruction for a correspondence file is "Destroy after 3 years," then destroy it 3 years after the annual cutoff date has been reached.

DL1.1.26.3. For records with retention periods based on an event or action. Cut off on the date the event occurs or the action is completed, and then apply the retention period. For example, if the disposition for case working papers is "Destroy when related case file is closed," then cut off and destroy the working papers when closing the related file.

DL1.1.26.4. For records with retention periods based on a specified time period after an event or action. Place in an inactive file on the date the event occurs or the action is completed and cut off the inactive file at the end of each fiscal (or calendar) year; then apply the retention period. For example, if the disposition for a case file is "Destroy 6 years after case is closed," then destroy 6 years after the annual cutoff along with all other case files closed during that year.

DL1.1.27. Cycle. The periodic replacement of obsolete copies of vital records with copies of current vital records. This may occur daily, weekly, quarterly, annually, or at other designated intervals as specified by regulation or by the records manager (see 36 CFR 1236.14, reference (f)).

DL1.1.28. DoD Discovery Metadata Specification (DDMS). The Department of Defense Discovery Metadata Specification defines discovery metadata elements for resources posted to community and organizational shared spaces. The DDMS specifies a set of information fields that are to be used to describe any data or service asset that is made known to the Enterprise.

DL1.1.29. Database. In electronic records, a set of data elements, consisting of at least one file or of a group of integrated files, usually stored in one location and made available to several users (see 36 CFR 1234.2, reference (g)).

DL1.1.30. Database Management System (DBMS). A software system used to access and retrieve data stored in a database (see reference (g)).

DL1.1.31. Data Element. A combination of characters or bytes that refers to a single piece of information, such as name, address, or age (see Instructional Guide, reference (h)).

DL1.1.32. Date Filed. The date and time that an electronic document was filed in the RMA and declared a record. This date and time will be assigned by the computer at the time the record is filed in the RMA.

DL1.1.33. Declassification. The authorized change in the status of information from classified information to unclassified information (see reference (d)).

DL1.1.34. Declassification Guide. Written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified (see reference (d)).

DL1.1.35. Defense Message System (DMS). A secure and accountable writer–to-reader messaging service accessible from world-wide DoD locations to tactically deployed users and other designated Federal users, with interfaces to Allied users and Defense contractors.

DL1.1.36. Delete. The process of permanently removing, erasing, or obliterating recorded information from a medium, especially a reusable magnetic disk or tape (see reference (h)).

DL1.1.37. Denial Authority. Name, title, position, and signature or electronic signature of individual designated with permission to deny access to records requested under the Privacy Act, or FOIA.

DL1.1.38. Department of Defense (DoD) Components. The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense.

DL1.1.39. Derivative Classification. The incorporating, paraphrasing, restating or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification (see reference (d)).

DL1.1.40. Destruction. In records management, the primary type of disposal action. Methods of destroying records include selling or salvaging the record medium and burning, pulping, shredding, macerating, or discarding it with other waste materials (see 36 CFR 1228.58, reference (i)).

DL1.1.41. Disposition. Those actions taken regarding Federal records after they are no longer required to conduct current Agency business (see reference (e)). These actions include:

DL1.1.41.1. Transfer of records to Agency storage facilities or Federal Record Centers (FRCs).

DL1.1.41.2. Transfer of records from one Federal Agency to another.

DL1.1.41.3. Transfer of permanent records to the National Archives.

DL1.1.41.4. Disposal of temporary records no longer needed to conduct agency business, usually by destruction or, occasionally, by donation of temporary records to an eligible person or organization after the authorized retention period has expired and after NARA has approved the donation (see 36 CFR 1228.60, reference (j)).

DL1.1.42. Disposition Action. Action to be taken when a disposition date occurs (e.g., interim transfer, accession, or destroy).

DL1.1.43. Disposition Action Date. The fixed date on which the records in a file become due for final disposition.

DL1.1.44. Disposition Authority. Legal authority that empowers an Agency to transfer permanent records to the National Archives or to carry out the disposal of temporary records. Must be obtained from NARA and also, for certain records proposed as temporary, from the GAO (see reference (e)).

DL1.1.45. Disposition Instruction. Directions for cutting off records and carrying out their disposition (transfer, retirement, or destruction) in compliance with NARA's regulations and the General Records Schedule (GRS). Disposition instructions in an RMA include retention-related fields such as authority, transfer location, active or dormant chronological retention periods, and conditional retention periods (see reference (e)).

DL1.1.46. Disposition Instruction Type. One of three ways of scheduling a disposition instruction: time, event, or a combination of both time and event. See DL1.55., DL1.126., and DL1.127. (see also reference (e)).

DL1.1.47. Document. Information set down in any physical form or characteristic. A document may or may not meet the definition of a record.

DL1.1.48. Document Type Definition (DTD). A Document Type Definition is a set of declarations that conform to a particular markup syntax and that describe a class, or "type", of SGML or XML documents, in terms of constraints on the structure of those documents. A DTD specifies, in effect, the syntax of an "application" of SGML or XML, such as the derivative language HTML or XHTML. This syntax is usually a less general form of the syntax of SGML or XML.

DL1.1.49. Downgrade. A determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level (see reference (d)).

DL1.1.50. Drop-down Lists. A predefined set of data used to populate certain record metadata fields.

DL1.1.51. Dublin Core. The Dublin Core is a metadata element set. It includes all Dublin Core Metadata Initiative terms (that is, refinements, encoding schemes, and controlled vocabulary terms) intended to facilitate discovery of resources. The Dublin Core has been in development since 1995 through a series of focused invitational workshops that gather experts from the library world, the networking and digital library research communities, and a variety of content specialties.

DL1.1.52. Edit. Function that allows the user to change an existing record's metadata.

DL1.1.53. Electronic Mail Message. A document created or received via an electronic mail system, including brief notes, formal or substantive narrative documents, and any attachments, such as word processing and other electronic documents, which may be transmitted with the message (see reference (g)).

DL1.1.54. Electronic Mail System. A computer application used to create, receive, and transmit messages and other documents electronically. This definition does not include file transfer utilities (software that transmits files between users but that does not retain any transmission data); computer systems used to collect and process data organized into data files or databases; and word-processing documents not transmitted via an e-mail system (see reference (g)).

DL1.1.55. Electronic Record. Information recorded in a form that requires a computer or other machine to process it and that satisfies the legal definition of a record according to 44 U.S.C. 3301 (reference (k)).

DL1.1.56. Embedded Fonts. Technology that allows fonts used in the creation of a document to travel with that document, ensuring that a user sees documents exactly as the designer intended them to be seen.

DL1.1.57. Event Disposition. A disposition instruction in which a record is eligible for the specified disposition (transfer or destroy) upon or immediately after the specified event occurs. No retention period is applied and there is no fixed waiting period as with "timed" or combination "timed-event" dispositions. Example: "Destroy upon completion of General Accounting Office Audit" (see reference (e)).

DL1.1.58. Exemption Categories. List of specific reasons, as specified in EO 12958, as amended, that agency heads use to exempt classified material from automatic declassification.

DL1.1.59. Exchangeable Image File Format (EXIF) Information. The exchangeable image file format is a specification for the image file format used by digital cameras.

CL1.1.60. Extensibility. Extensibility is a system design principle where the implementation takes into consideration future growth. It is a systemic measure of the ability to extend a system and the level of effort required to implement the extension. Extensions can be through the addition of new functionality or through modification of existing functionality. The central theme is to provide for change while minimizing impact to existing system functions.

DL1.1.61. File. An arrangement of records.

DL1.1.61.1. When used as a noun, this term is used to denote papers, photographs, photocopies, maps, machine-readable information, or other recorded information, regardless of physical form or characteristic. Files are accumulated or maintained on shelves, in filing equipment, boxes, or machine-readable media, and they occupy office or storage space (see 36 CFR 1220.14, reference (l)).

DL1.1.61.2. When used as a verb, this term is used to define the act of assigning and storing records in accordance with the file plan (see reference (e)).

DL1.1.62. File Plan. A document containing the identifying number, title, description, and disposition authority of files held or used in an office (see reference (e)).

DL1.1.63. Format. For electronic records, format refers to the computer file format described by a formal or vendor standard or specification, such as ISO/IEC 8632-1 [Information Technology - Computer Graphics - Metafile for the Storage and Transfer of Picture Description Information (CGM)]; ISO/IEC 10918 [Joint Photographic Experts Group (JPEG)]; WordPerfect 6.1 for Windows; or Microsoft Word 7.0 for Windows. For non-electronic records, the format refers to its physical form: e.g., paper, microfilm, and video.

DL1.1.64. Freeze. The suspension or extension of the disposition of temporary records that cannot be destroyed on schedule because of special circumstances, such as a court order or an investigation. A freeze requires a temporary extension of the approved retention period (see reference (e)).

DL1.1.65. Global Information Grid (GIG). The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to Warfighters, policy makers and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve information superiority.

DL1.1.66. Government Information Locator Service (GILS). A Federal Government service to help the general public locate and access information throughout the Federal Government (see 44 U.S.C. 3511, reference (m)). GILS describes the information available in those resources and provides assistance in obtaining that information. GILS uses network technology and international standards for information search and retrieval. These standards are described in the Federal Information Processing Standard (FIPS) Publication 192, "Application Profile for the Government Information Locator Service" (reference (n)).

DL1.1.67. ICC/ICM Profile. Profile describing exactly how the primary colors map to device independent color.

DL1.1.68. Imaging Tools. Software and hardware that works together to capture, store, and recreate images.

DL1.1.69. Ingest. Ability of an RMA to bring in exported records and record metadata.

DL1.1.70. Inheritance. Field inherits data from the same field in the parent object.

DL1.1.71. Intelligent Name. Intelligent names are clear, uncoded, identifications of the individual.

DL1.1.72. Interdependent Fields. Values placed in one field have an affect on what related fields are mandatory or what data can be entered into those fields.

DL1.1.73. Interoperability. The ability of systems, units, or forces to provide services to and accept services from other systems, units or forces and to use the services so exchanged to enable them to operate effectively together.

DL1.1.74. Keyboard Shortcut. A keyboard shortcut (also known as an accelerator key, shortcut key, or hotkey) is one or a set of keyboard keys that, when pressed simultaneously, perform a predefined task. Such a task could be done with the computer's pointing device, but would require the user to take his or her hands off of the keyboard, and then place them on said device. Hence, they are a shortcut in that they save the user time.

DL1.1.75. Life Cycle. The records life cycle is the life span of a record from its creation or receipt to its final disposition. It is usually described in three stages: creation, maintenance and use, and final disposition.

DL1.1.76. Lifecycle Phase. A specific phase of a record’s existence from creation through final disposition.

DL1.1.77. Linking. Referencing or associating records with one another.

DL1.1.78. Location of Record. A pointer to a record’s location. Examples: an operating system path and filename, the location of a file cabinet, or the location of a magnetic tape rack.

DL1.1.79. Marginalia. Marginalia is the general term for notes, scribbles, doodles and editorial comments made in the margin of a book. Marginalia can add or detract from the value of a book, depending on the book and the author of the marginalia

DL1.1.80. Media Type. The material or environment on which information is inscribed (e.g., microform, electronic, paper).

DL1.1.81. Move. Function that allows the user to relocate records and metadata.

DL1.1.82. Multiple Sources. Information classified based on two or more source documents, classification guides or combination of both (see reference (d)).

DL1.1.83. Namespace. An XML namespace is a W3C standard for providing uniquely named elements and attributes in an XML instance. An XML instance may contain element or attribute names from more than one XML vocabulary. If each vocabulary is given a namespace then the ambiguity between identically named elements or attributes can be resolved. All element names within a namespace must be unique.

DL1.1.84. Office Applications. Software packages that perform a variety of office support functions, such as word processing, desktop publishing, spreadsheet calculations, electronic mail, facsimile transmission and receipt, document imaging, optical character recognition (OCR), workflow, and data management. These applications are generally used to generate, convert, transmit, or receive business documents.

DL1.1.85. Optical Character Recognition (OCR). OCR is the recognition of printed or written text characters by a computer. This involves analysis of the scanned-in image, and then translation of the character image into character codes, such as ASCII. OCR is being applied by libraries, businesses, and government agencies to create text-searchable files for digital collections. OCR is also used to help process checks and credit card slips and sort the mail.

DL1.1.86. Original Classification. An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure (see reference (d)).

DL1.1.87. Originating Organization. Official name or code identifying the office responsible for the creation of a document.

DL1.1.88. Permanent Record. Records appraised by NARA as having sufficient historical or other value to warrant continued preservation by the Federal Government beyond the time they are normally needed for a particular Agency's administrative, legal, or fiscal purposes (see reference (e)).

DL1.1.89. PKI-enabled. Allows for the secure exchange of data over otherwise unsecured media.

DL1.1.90. Portal. A single point of access for all repositories and databases storing electronic records and record metadata.

DL1.1.91. Producing Applications. Software that feeds records into the RMA.

DL1.1.92. Product Combinations. The result of integrating two or more distinct products, where typically, one product primarily creates records and another product performs the records' retention schedule tracking.

DL1.1.93. Privileged Users. Individuals who are given special permission to perform functions beyond those of typical users.

DL1.1.94. Publication Date. The date and time that the author or originator completed the development of or signed the document. For electronic documents, this date and time should be established either by the author or from the time attribute assigned to the document by the application used to create the document. This is not necessarily the date or time that the document was filed in the RMA.

DL1.1.95. Public Key Infrastructure (PKI). PKI is an arrangement that provides for third party vetting of, and vouching for, user identities. It also allows binding of public keys to users. This is usually carried out by software at a central location together with other coordinated software at distributed locations. The public keys are typically in certificates.

DL1.1.96. Rebuild. Reconstructing the RM environment after a disaster.

DL1.1.97. Receipt Data. Information in electronic mail systems regarding dates and times of receipt of a message, or acknowledging receipt or access by specific addressee(s). It is not the date and time of delivery to the Agency. If receipt data are provided by the computer system, they are a required part of documents or records received through electronic mail (see reference (g)).

DL1.1.98. Record. Information, regardless of medium, detailing business transactions. Records include all books, papers, maps, photographs, machine-readable materials, and other documentary materials, regardless of physical form or characteristics. Records are made or received by an Agency of the United States Government under Federal law or in connection with the transaction of public business. Records are preserved or appropriate for preservation by that Agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the value of data in the record (see reference (k)).

DL1.1.99. Record Category. A description of a particular set of records within a file plan. Each category has retention and disposition data associated with it, applied to all record folders and records within the category.

DL1.1.100. Record Category Identifier. An Agency's alphanumeric or numeric identifier indicating a unique record category.

DL1.1.101. Record Element. A logical data structure comprised of embedded record elements and record attributes.

DL1.1.102. Record Folder. A record folder is an extension to the file plan either as a static structure or an aggregate gathering of records. It is used to manage case records and to break other records into periods supporting retention and disposition.

DL1.1.103. Record Identifier. An element of metadata, a record identifier is a data element whose value is system-generated and that uniquely identifies a particular record.

DL1.1.104. Records Management. The planning, controlling, directing, organizing, training, promoting, and other managerial activities involving the life cycle of information, including creation, maintenance (use, storage, retrieval), and disposal, regardless of media. Record management procedures are used to achieve adequate and proper documentation of Federal policies and transactions and effective and economical management of Agency and organizational operations (see 44 U.S.C. 2901, reference (o)).

DL1.1.105. Records Management Application (RMA). Software used by an organization to manage its records. An RMA's primary management functions are categorizing and locating records and identifying records that are due for disposition. RMA software also stores, retrieves, and disposes of the electronic records that are stored in its repository.

DL1.1.106. Records Managers. Individuals who are responsible for records management administration.

DL1.1.107. Record Metadata. Data describing data; that is, data describing the structure (data elements), interrelationships, and other characteristics of records.

DL1.1.108. Recovery/Rollback Capability. Ability to re-establish the system following any system failure.

DL1.1.109. Redaction. Separation of disclosable from non-disclosable information by removing or permanently blocking out individual words, sentences or paragraphs, or the removal of whole pages prior to the release of the document..

DL1.1.110. Referential Integrity. Ensuring that all references are updated or deleted as necessary when a key reference is changed in a database environment.

DL1.1.111. Regrade. A determination by a classification or declassification authority that information classified and safeguarded at a specified level requires a different level of classification and safeguarding.

DL1.1.112. Relational Integrity. Ensuring that "children" in a database or hierarchical structure are updated or deleted appropriately as actions are taken on the "parent." Maintaining relational integrity prevents "orphans."

DL1.1.113. Rendering Aid. Provides the capability to properly render and present metadata content and context.

DL1.1.114. Rendition. Replication that provides the same content but differs from the reference because of storage format, or storage medium.

DL1.1.115 Repository for Electronic Records. A direct access device on which the electronic records and associated metadata are stored.

DL1.1.116. Retention Period. The length of time that a record must be kept before it can be destroyed. Records not authorized for destruction are designated for permanent retention. Retention periods for temporary records may be expressed in two ways (see reference (e)).

DL1.1.116.1. A fixed period from the time records in the series or system is created. Normally, a fixed period that follows their regular cutoff dates. For example, the phrase "destroy after 2 years" provides continuing authority to destroy records in a given series 2 years after their creation (normally 2 years after their regular cutoff date).

DL1.1.116.2. A fixed period after a predictable event. Normally, a fixed period following the systematic cutoff applied after completion of an event. The wording in this case depends on the kind of action involved. Note the following examples:

DL1.1.116.2.1. "After completion" (as of a study, project, audit).

DL1.1.116.2.2. "After sale or transfer" (as of personal or real property).

DL1.1.116.2.3. "After publication" (as of monthly reports).

DL1.1.116.2.4. "After superseded" (as of an administrative directive).

DL1.1.116.2.5. "After revision or cancellation" (as of a form).

DL1.1.116.2.6. "After acceptance or rejection" (as of an application).

DL1.1.117. Retention Schedule: A plan for the management of records listing types of records and how long they should be kept; the purpose is to provide continuing authority to dispose of, transfer, or archive records.

DL1.1.118. Roles. Grouping of resource permissions defined for an application.

DL1.1.119. Scheduled Records. Records whose final disposition has been approved by NARA.

DL1.1.120. Screening. Aggregating and reviewing records for management and disposition purposes.

DL1.1.121. Service-oriented Architecture (SOA). A service-oriented architecture is essentially a collection of services. These services communicate with each other. The communication can involve either simple data passing or it could involve two or more services coordinating some activity. Some means of connecting services to each other is needed.

DL1.1.122. Source Document. An existing document that contains information that is incorporated, paraphrased, restated, or generated in new form into a new document (see reference (d)).

DL1.1.123. Standardized Data Element. Data elements clearly defined by data type and size.

DL1.1.124. Storage. Space for non-active records. Can be digital, optical, or cubic feet.

DL1.1.125. Subject. The principal topic addressed in a record.

DL1.1.126. Supplemental Markings. Document markings not necessarily related to classification markings, but which elaborate on or clarify document handling, e.g., "ORCON (Originator Controlled);" Special Access Programs; "RD (Restricted Data)."

DL1.1.127. System of Records. A group of records under the control of any agency from which information is retrieved by the name of the individual or by an individual identifier.

DL1.1.128. Time Disposition. A disposition instruction specifying when a record shall be cut off and when a fixed retention period is applied. The retention period does not begin until after the records have been cut off. Example: "Destroy after 2 years — cut off at the end of the calendar (or fiscal) year; hold for 2 years; then destroy" (see reference (e)).

DL1.1.129. Time-Event Disposition. A disposition instruction specifying that a record shall be disposed of at a fixed period of time after a predictable or specified event. Once the specified event has occurred, then the retention period is applied. Example: "Destroy 3 years after close of case." The record does not start its retention period until after the case is closed — at that time its folder is cutoff and the retention period (destroy after 3 years) is applied (see reference (e)).

DL1.1.130. Transfer. The act or process of moving records from one location to another, especially from the office space in which the record is used, to Agency storage facilities or FRCs, from one Federal Agency to another, or from office or storage space to the National Archives for permanent preservation. Transfer does not relieve the owning organization of legal and management responsibilities for non-permanent records. Accessioning permanent records to NARA does transfer legal ownership and responsibility for the records to NARA (see reference (e)).

DL1.1.131. Transmission Data. Information in electronic mail systems regarding the date and time messages were sent or forwarded by the author or originator. If this data is provided by the electronic mail system, it is required as part of the record for documents that are transmitted and received via electronic mail (see reference (g)).

DL1.1.132. Trigger. Database triggers are procedures that are stored in a database and are executed or "fired" when a table is modified. They are very powerful tools that can be used to perform many tasks such as restricting access to specific data, perform logging, or auditing of data sets.

DL1.1.133. Unscheduled Records. Records that do not have a NARA-approved final disposition.

DL1.1.134. Upgrade. A determination that certain information requires, in the interest of national security, a higher degree of protection against unauthorized disclosure than currently provided, together with a changing of the classification designation to reflect such higher degree. The determination to reclassify information pursuant to to EO 12958 as amended by EO 13292 (reference (d)) is a form of classification upgrade for the purposes of this standard.

DL1.1.135. User-Definable Fields. Fields defined during application configuration by authorized individuals to support organization-specific information management and access requirements.

DL1.1.136. Version. One of a sequence of documents having the same general form and specific subject and purpose. The sequence often reflects successive changes to a document.

DL1.1.137. View. Function that allows the user to look at the metadata and content of a record in a viewer or other application.

DL1.1.138. Vital Records. Essential Agency records needed to meet operational responsibilities under national security emergencies or other emergency or disaster conditions (emergency operating records) or to protect the legal and financial rights of the Government and those affected by Government activities (legal and financial rights records). They are subject to periodic review and update. Emergency operating records are the type of vital records essential to the continued functioning or reconstitution of an organization during and after an emergency. Included are emergency plans and directive(s), orders of succession, delegations of authority, staffing assignments, selected program records needed to continue the most critical Agency operations, and related policy or procedural records assisting Agency staff in conducting operations under emergency conditions and for resuming normal operations after an emergency. Legal and financial rights records are those essential to protecting the legal and financial rights of the Government and of the individuals directly affected by its activities. Examples include accounts receivable records, social security records, payroll records, retirement records, and insurance records. These records were formerly defined as "rights-and-interests" records (see reference (f)).

DL1.1.139. Workflow. The tasks, procedural steps, organizations or people, required input and output information, and tools needed for each step in a business process. A workflow approach to analyzing and managing a business process can be combined with an object-oriented programming approach, which tends to focus on documents, data, and databases.

DL1.1.140. Extensible Stylesheet Language Transformations (XSLT). XSLT specifies the styling of an XML document by describing how one XML document is transformed into another XML document.

DL1.1.141. XML Schema. An XML schema is a description of a type of XML document, typically expressed in terms of constraints on the structure and content of documents of that type, above and beyond the basic syntax constraints imposed by XML itself. An XML schema provides a view of the document type at a relatively high level of abstraction.

AL1.1. ABBREVIATIONS AND ACRONYMS

AL1.1.1.	AISs	Automated Information Systems
AL1.1.2.	ASD	Assistant Secretary of Defense
AL1.1.3.	C4ISR	Command, Control, Communications, Computers and Intelligence Surveillance and Reconnaissance
AL1.1.4.	CAC	Common Access Card
AL1.1.5.	CFR	Code of Federal Regulations
AL1.1.6.	CGM	Computer Graphics Metafile
AL1.1.7.	CIO	Chief Information Officer
AL1.1.8.	COFF	Cutoff
AL1.1.9.	COTS	Commercial-off-the-Shelf
AL1.1.10.	DASD	Deputy Assistant Secretary of Defense
AL1.1.11.	DBMS	Database Management System
AL1.1.12.	DCID	Director of Central Intelligence Directive
AL1.1.13.	DISA	Defense Information Systems Agency
AL1.1.14.	DDMS	DoD Discovery Metadata Specification
AL1.1.15.	DMS	Defense Message System
AL1.1.16.	DoD	Department of Defense
AL1.1.17.	DoDD	Department of Defense Directive
AL1.1.18.	DDMS	Department of Defense Discovery Metadata Specification
AL1.1.19.	DTD	Document Type Definition
AL1.1.20.	EO	Executive Order
AL1.1.21.	E-mail	Electronic mail
AL1.1.22.	EXIF	Exchangeable Image File Format
AL1.1.23.	FIPS	Federal Information Processing Standard
AL1.1.24.	FOIA	Freedom of Information Act
AL1.1.25.	FRC	Federal Records Center
AL1.1.26.	GAO	General Accounting Office
AL1.1.27.	GIF	Graphic Image Format
AL1.1.28.	GIG	Global Information Grid
AL1.1.29.	GILS	Government Information Locator Service
AL1.1.30.	GRS	General Records Schedule
AL1.1.31.	IAR	Individual Access Request
AL1.1.32.	ICC/ICM	International Color Consortium/Image Color Management
AL1.1.33.	IM	Information Management
AL1.1.34.	ISO	International Standards Organization
AL1.1.35.	IT	Information Technology
AL1.1.36.	JITC	Joint Interoperability Test Command
AL1.1.37.	JPEG	Joint Photographic Experts Group
AL1.1.38.	JTA	Joint Technical Architecture
AL1.1.39.	LAN	Local Area Network
AL1.1.40.	NARA	National Archives and Records Administration
AL1.1.41.	NOS	Network Operating System

AL1.1.42.	NSS	National Security Systems
AL1.1.43.	OCR	Optical Character Recognition
AL1.1.44.	OLE	Object Linking and Embedding
AL1.1.45.	OSD	Office of the Secretary of Defense
AL1.1.46.	PKI	Public Key Infrastructure
AL1.1.47.	PNG	Portable Network Graphics
AL1.1.48.	RM	Records Management
AL1.1.49.	RMA	Records Management Application
AL1.1.50.	RMTF	Records Management Task Force
AL1.1.51.	SMTP	Simple Mail Transfer Protocol
AL1.1.52	sRGB	Standard Red Green Blue
AL1.1.53.	SOR	System of Records
AL1.1.54.	SORN	System of Records Notice
AL1.1.55	STD	Standard
AL1.1.56.	TCP/IP	Transmission Control Protocol/Internet Protocol
AL1.1.57.	TIFF	Tagged Image Interchange Format
AL1.1.58.	UCNI	Unclassified Controlled Nuclear Information
AL1.1.59.	UDDI	Universal Description Discovery and Integration
AL1.1.60.	U.S.C.	United States Code
AL1.1.61.	WAN	Wide Area Network
AL1.1.62.	XML	eXtensible Markup Language

C1. CHAPTER 1

GENERAL INFORMATION

C1.1. PURPOSE

C1.1.1. This standard sets forth mandatory baseline function requirements and requirements for classified marking, access control, and other issues, and identifies non-mandatory features deemed desirable for Records Management Application (RMA) software. This revised version of the standard incorporates requirements for managing Freedom of Information Act and Privacy Act records. This version also incorporates baseline requirements for RMA-RMA interoperability and archival transfer to the National Archives and Records Administration (NARA).

C1.1.2. This standard describes the minimum records management requirements that must be met in accordance with 44 U.S.C. 2902 (reference (p)) and guidance and implementing regulations promulgated by NARA. The word "shall" identifies mandatory system standards and the word "should" identifies design objectives that are desirable but not mandatory.

C1.1.3. This version also encourages the development of RMA software to adhere to DoD net-centric information sharing principles. The Department of Defense’s (DoD) Components, Services, and Agencies will use this Standard in the implementation of their records management programs. References (bc) and (bd) detail the DoD’s information sharing principles, identifying the need to make data holdings visible, accessible, understandable, and trusted. The DoD’s records are an important part of the DoD’s information assets, and as such should be included in efforts to improve information sharing. New requirements found in this standard are intended to ensure that for the DoD, RMA software will facilitate DoD Components’, Services’, and Agencies’ efforts to share information in this way. The goal of this standard relative to the DoD’s records is to make records: (1) visible by developing and registering standardized metadata, (2) accessible through web services with usable, standardized interfaces, and (3) understandable through the availability and use of rich metadata describing the records and their context.

C1.1.4. As part of the DoD’s movement towards net-centric information sharing, RMA software should migrate towards providing standards-compliant services for the DoD. These services would provide the capability to announce an RMA’s holdings and request records, making records both visible and accessible. The services would be paired with with service connection instructions, making the service itself understandable. DoD users of RMA software would then incorporate these services into a larger service oriented architecture to achieve broader information sharing.

C1.2. LIMITATIONS

This Standard addresses a minimum set of baseline functional requirements applicable to all RMAs used within the Department of Defense. For the Defense Information Systems Agency's (DISA) Joint Interoperability Test Command (JITC) to certify that an RMA is compliant with this Standard, these minimum requirements must be met, regardless of organizational and site-specific needs. Using organizations may identify additional requirements to satisfy their site-specific needs, but these functions will not be tested nor certified as compliant by JITC. Some examples of site-specific needs are the capability to capture and manage Defense Messaging System (DMS) records, and the capability of adopting features described as optional in Chapter 3 of this Standard. These requirements will be addressed in a later version of this Standard.

(This page intentionally left blank.)

C2. CHAPTER 2

MANDATORY REQUIREMENTS

C2.1. GENERAL REQUIREMENTS

C2.1.1. Managing Records. RMAs shall manage records in accordance with this Standard, regardless of storage media or other characteristics (see 44 U.S.C. 3103 and 36 CFR 1222.10, references (q) and (r)).

C2.1.2. Accommodating Dates and Date Logic. RMAs shall correctly accommodate and process information that contains dates in current, previous, and future centuries (see ISO 8601, reference (s)). The capability shall include, but not be limited to, century recognition, calculation, and logic that accommodate same century and multi-century formulas and date values, and date interface values that reflect the century. RMAs shall store years in a 4-digit format. Leap year calculations shall be accommodated (e.g., 1900 is not a leap year; 2000 is a leap year).

C2.1.3. Metatagging Organizational Data. RMAs shall allow for the implementation of discovery metatagging. Current guidance for metatagging DoD data can be found in the Department of Defense Discovery Metadata Specification (reference (c)).When selecting commercial-off-the-shelf (COTS) products to support RMA requirements, selection criteria should include the feasibility and capability of the COTS products to implement and maintain DoD discovery metadata requirements. This requirement implies the capability for adding user-defined metadata fields, modifying existing field labels, and mapping data fields to standard transfer format fields.

C2.1.4. Backward Compatibility. RMAs shall provide the capability to access information from their superseded repositories and databases. This capability shall support at least one previously verified version of backward compatibility.

C2.1.5. Accessibility. The available documentation for RMAs shall include product information that describes features that address 36 CFR 1194.21 and 1194.31 (references (t) and (u)). For web-based applications, 36 CFR 1194.22 (reference (v)) shall also apply (see 29 U.S.C. 794d, reference (w)).

C2.1.6. Extensibility. RMAs shall include the capability to integrate the RMA into an organization’s information technology enterprise. This capability shall include the capability to accept and file records from producing applications and provide support to the organization’s workflow.

C2.2. DETAILED REQUIREMENTS

C2.2.1. Implementing File Plans.

C2.2.1.1. RMAs shall provide the capability for only authorized individuals to create, edit, and delete file plan components and their identifiers. Each component identifier shall be linked to its associated component and to its higher-level component identifier(s) (see 44 U.S.C. 3303 and 36 CFR 1222.50, references (x) and (y)). Mandatory file plan components are shown in Table C2.T.1. Mandatory Data Collection indicates that RMAs shall ensure population of the associated data structure with non-null values. For fields that are not mandatory Data Collection column, RMAs shall behave in a predictable manner as a result of queries or other operations when the fields are not populated. Mandatory Data Structure indicates that the field must be present and available to the user either as read/write or as read only depending upon the kind of data being stored. Mandatory Support indicates that the RMA shall support capability without undue constraint. The file plan components should be organized into logical sets that, when populated, will provide all the file plan references necessary to properly annotate (file) a record.

Table C2.T1. File Plan Components

Requirement	**File Plan Component**	**Reference/ Comment**
Mandatory Data Collection		
C2.T1.1.	Record Category Name	RMTF (reference (z))
C2.T1.2.	Record Category Identifier	RMTF (reference (z))
C2.T1.3.	Record Category Description	RMTF (reference (z))
C2.T1.4.	Disposition Instructions	36 CFR 1228.24 (reference (aa))
C2.T1.5.	Disposition Authority	RMTF (reference (z))
C2.T1.6	Transfer or Accession to NARA Indicator	
C2.T1.7.	Vital Record Indicator	36 CFR 1236.20 (reference (ab))
Mandatory Data Structure		
C2.T1.8.	Vital Record Review and Update Cycle Period	36 CFR 1236.20 reference (ab))
Mandatory Support		
C2.T1.9.	User Definable Fields	Multiple user defined fields shall be supported

C2.2.1.2. RMAs shall provide the capability for authorized individuals to designate the metadata fields that are to be constrained to selection lists. RMAs shall provide the capability for authorized individuals to create and maintain selection lists for all supported data types (e.g., drop-down lists) for metadata items that are constrained to a pre-defined set of data.

C2.2.1.3. RMAs shall provide the capability for only authorized individuals to create, edit, and delete file plan metadata elements or attributes, and their associated selection lists.

C2.2.1.4. RMAs shall provide the capability for authorized individuals to select where data collection for optional metadata fields is mandatory for a given organization.

C2.2.1.5. RMAs shall provide the capability for only authorized individuals to create, edit, and delete record folder components and their non-system generated identifiers. Each component identifier shall be linked to its associated component and to its higher-level file plan component identifier(s) (see references (t) and (y)). Mandatory record folder components are shown in Table C2.T2. Mandatory Data Collection indicates that RMAs shall ensure population of the associated data structure with non-null values. For fields that are not mandatory Data Collection column, RMAs shall behave in a predictable manner as a result of queries or other operations when the fields are not populated. Mandatory Inheritance Support indicates that the field must inherit data from the same field in the parent object and may be locally overwritten. Mandatory Data Structure indicates that the field must be present and available to the user either as read/write or as read only depending upon the kind of data being stored. Mandatory Support indicates that the RMA shall support capability without undue constraint. If the RMA requires the use of folders for all categories, it must be able to accommodate record level retention schedules without requiring the user to create a folder for each record.

Table C2.T2. Record Folder Components

Requirement	**File Plan Component**	**Reference/ Comment**
Mandatory Data Collection		
C2.T2.1.	Folder Name	
C2.T2.2.	Folder Unique Identifier	
C2.T2.3.	Location	RMTF (reference (z))
Mandatory Inheritance Support		
C2.T2.4.	Vital Record Indicator	36 CFR 1236.20 (reference (ab))
Mandatory Data Structure		
C2.T2.5.	Vital Record Review and Update Cycle Period	36 CFR 1236.20 (reference (ab))
C2.T2.6.	Supplemental Marking List	Multiple supplemental marking entry selections shall be supported.
Mandatory Support		
C2.T2.7.	User Definable Fields	Multiple user definable fields shall be supported

C2.2.1.6. RMAs shall provide the capability for only authorized individuals to create, edit, and delete folder metadata elements or attributes, and their associated selection lists.

C2.2.1.7. RMAs shall provide the capability for authorized individuals to select where data collection for optional metadata fields is mandatory for a given organization.

C2.2.1.8. RMAs shall ensure that identifiers (e.g., folder identifiers, record category identifiers) are unique so that ambiguous assignments, links, or associations cannot occur.

C2.2.1.9. RMAs shall provide the capability to associate the attributes of file plan components to record folders and records where the records are not associated with folders.

C2.2.1.10. RMAs shall provide a scripting capability to only authorized individuals that allow them to attach simple process actions such as alerts and notifications to any or all metadata fields or to restrict record access based on the content of fields. This scripting capability shall allow for evaluation of the contents of two or more fields on the same record as well as fields in objects linked to that record.

C2.2.1.11. RMAs shall provide the capability to sort by one or multiple fields, view, save, and print user-selected portions of the file plan, including record folders (see reference (z)).

C2.2.2. Scheduling Records.

C2.2.2.1. RMAs shall provide the capability for only authorized individuals to create, edit, and delete retention schedule components of record categories.

C2.2.2.2. RMAs shall provide the capability for defining an unconstrained number of multiple phases (e.g., transfer to inactive on-site storage, transfer to off-site storage) within a retention schedule.

C2.2.2.3. RMAs shall provide the capability for defining parallel and interdependent phases within a retention schedule, including the capability for assigning phase precedence or weight.

C2.2.2.4. RMAs shall allow an authorized individual to select cutoff as the trigger to begin final disposition calculations.

C2.2.2.5. RMAs shall calculate interim phases and final disposition from the trigger date selected by an authorized individual.

C2.2.2.6. RMAs shall provide the capability for only authorized individuals to define the cutoff criteria and, for each life cycle phase, define the following disposition components for a record category:

C2.2.2.6.1. Retention Period (e.g., fiscal year).

C2.2.2.6.2. Disposition Action (interim transfer, accession, or destroy).

C2.2.2.6.3. Interim Transfer or Accession Location (if applicable).

C2.2.2.7. RMAs shall, as a minimum, be capable of scheduling and rescheduling each of all records and/or record folders. Mandatory disposition types include:

C2.2.2.7.1. Time Dispositions, cyclical process where records are eligible to enter their disposition lifecycle immediately after the conclusion of a fixed period of time following user-defined cutoff (e.g., days, months, years).

C2.2.2.7.2. Event Dispositions, unique event(s) process where records are eligible for disposition immediately after a specified event takes place (i.e., event acts as cutoff and there is no retention period).

C2.2.2.7.3. Time-Event Dispositions, unique event(s) process where the timed retention periods are triggered after a specified event takes place (i.e., event makes the record folder eligible for closing and/or cutoff and there is a retention period).

C2.2.2.8. RMAs shall allow authorized individuals the capability of defining and naming disposition events. Multiple events per disposition instruction shall be supported with one or more being necessary to trigger cutoff, retention and/or interim transfer actions as required by the organization. RMAs shall support recurring events.

C2.2.2.9. RMAs shall provide the capability to automatically calculate the complete life cycle, including intermediate phases, of record folders and records not in folders (see reference (e)). RMAs shall allow an authorized individual to enter an “as-of” reference date for this calculation.

C2.2.2.10. RMAs shall provide the capability for rescheduling dispositions of record folders and/or records (those not in folders) during any phase of their life cycle if an authorized individual changes the disposition instructions. This requirement includes the capability to change the cutoff criteria of disposition instructions and to change the retention period(s) associated with a disposition.

C2.2.2.11. The RMA shall provide recalculation of the record life cycle based on changes to any life-cycle date and set the filing status (i.e., open, closed) of the folder according to the business rules associated with date change(s).

C2.2.3. Declaring and Filing Records.

C2.2.3.1. RMAs shall provide the capability to associate the attributes of a record folder to a record, or, if implemented, for categories to be managed at the record level, provide the capability to associate a record category to a record (see reference (y)).

C2.2.3.2. Mandatory record metadata components are shown in Table C2.T3. Mandatory Structure indicates that the field shall be present and available to the user either as read/write or as read only depending upon the kind of data being stored. Mandatory Data Collection indicates that RMAs shall ensure population of the associated data structure with non-null values. Mandatory Support indicates that the RMA shall provide a capability to support creating and managing the metadata. Where data collection is not mandatory, RMAs shall behave in a predictable manner as a result of queries or other operations when the fields are not populated.

Table C2.T3. Record Metadata Components

Requirement	Record Metadata Component	Reference/Comment
Mandatory Data Collection		
	Record Identifiers, Markings, and Indicators	
C2.T3.1.	Unique Record Identifier	
	Record Descriptors	
C2.T3.2.	Subject or Title	36 CFR 1234.22 (reference (ac))
	Record Dates	
C2.T3.3.	Date Filed	RMTF (reference (z))
C2.T3.4.	Publication Date	36 CFR 1234.22 (reference (ac))
	Record People and Organizations	
C2.T3.5.	Author or Originator	36 CFR 1234.22 (reference (ac))
C2.T3.6.	Originating Organization	36 CFR 1234.22 (reference (ac))
Mandatory Data Structure		
	Record Identifiers, Markings, and Indicators	
C2.T3.7.	Supplemental Marking List	Multiple Supplemental Markings entry selections shall be supported (see DCID 6/6, DoD Directive 5210.83, DoD 5400.7-R, DoD Directive 5230.24, and DoD 5200.1-R, references (ad), (ae), (af), (ag), and (ah))
	Record Descriptors	
C2.T3.8.	Media Type	RMTF (reference (z))
C2.T3.9.	Format	RMTF (reference (z))
	Record Dates	
C2.T3.10.	Date Received	
	Record People and Organizations	
C2.T3.11.	Addressee(s)	Mandatory for correspondence
C2.T3.12.	Other Addressee(s)	Mandatory for correspondence EO 12958, 36 CFR 1234.22, and DoD 5200.1-R, references (d), (ac), and (ah))
	Additional Metadata	
C2.T3.13.	Location	RMTF (reference (z))
Mandatory Support		
C2.T3.14.	User-Defined Fields	Multiple User-Defined Fields shall be supported

C2.2.3.3. RMAs shall provide the capability for only authorized individuals to create, edit, and delete record metadata elements or attributes, and their associated pick lists. RMAs shall provide a capability for only authorized individuals to indicate whether the field is constrained to a pick list and whether users can select more than one item from the list.

C2.2.3.4. RMAs shall provide the capability for authorized individuals to select where data collection for optional metadata fields is mandatory for a given organization.

C2.2.3.5. RMAs shall assign a unique computer-generated record identifier for each record they manage regardless of where that record is stored (see reference (z)).

C2.2.3.6. RMAs shall provide the capability to create, view, save, and print the complete record metadata, or user-specified portions thereof, sorted and/or grouped by user preference (see reference (z)).

C2.2.3.7. RMAs shall prevent subsequent changes to electronic records stored in its supported repositories. The content of the record, once filed, shall be preserved (see references (y) and (z)).

C2.2.3.8. RMAs shall not permit modification of the metadata fields indicated by this Standard as not editable.

C2.2.3.9. RMAs shall (for all records) capture, populate, and/or provide the user with the capability to populate the metadata elements before filing the record. RMAs shall ensure that fields designated mandatory for data collection are non-null before filing the record (see references (y) and (ac)).

C2.2.3.10. For records that are being filed via the user interface, RMAs shall provide the user with the capability to edit the record metadata prior to filing the record, except for data specifically identified in this Standard as not editable. For autofiling, RMAs shall provide the user the option of editing the record metadata prior to filing.

C2.2.3.11. Dates captured electronically shall be valid dates as defined in paragraph C2.1.2. Where data entry/capture errors are detected, RMAs shall prompt the user to correct the error. These prompts shall provide guidance to the user in making corrective actions; for example, "Date format incorrect - use YYYY/MM/DD."

C2.2.3.12. RMAs shall restrict the capability to only authorized individuals to define and add user-defined metadata fields (e.g., project number, budget line) for site-specific requirements (see reference (ac)).

C2.2.3.13. RMAs shall provide the capability to view, save, or print the metadata, including file plan and folder metadata, associated with a specified record or set of records, or user-specified portions thereof sorted and/or grouped by user preference.

C2.2.3.14. RMAs shall provide the capability for only authorized individuals to limit the record folders and record categories presented to a user or workgroup. Based on these limits, RMAs shall present to users only those record categories or folders available to the user or workgroup for filing.

C2.2.3.15. RMAs shall provide the capability for only authorized individuals to limit the selection or pick list items presented to a user or workgroup. Based on these limits, RMAs shall present to users only selection or pick list items available to the user or workgroup for filing.

C2.2.3.16. RMAs shall provide the capability for only authorized individuals to change a record folder or record category associated with a record.

C2.2.3.17. RMAs shall provide a capability for referencing or linking and associating supporting and related records and related information, such as notes, marginalia, attachments, and electronic mail-return receipts, etc., to a specified record. RMAs shall allow only authorized individuals to change or delete links and associations that affect disposition (see reference (z)).

C2.2.3.18. RMAs shall provide a capability for links to be labeled to indicate the type of relationship between the records, as well as to indicate the direction of the relationship. For example in a supersedes/superseded relationship, a later record supersedes an earlier one, and the earlier one was superseded by the later one, i.e. the label of the link from the later record to the earlier one should be “supersedes”, while the label of the link from the earlier record to the later one should be “superseded by”.

C2.2.3.19. RMAs shall provide a capability for the linking and unlinking of records both during and after the process of filing a record. RMAs shall allow only authorized individuals to remove links that affect disposition.

C2.2.3.20. RMAs shall provide a capability for authorized individuals to define, update, and assign permissions for use of user-defined link types (see reference (z)).

C2.2.3.21. RMAs shall provide the capability to support multiple renditions of a record. These shall be associated and linked. Each rendition shall be associated with its own set of metadata.

C2.2.3.22. RMAs shall provide the capability to increment versions of records when filing. RMAs shall associate and link the versions. Each version shall be associated with its own set of metadata.

C2.2.3.23. RMAs shall link the record metadata to the record so that it can be accessed for display, export, etc. (see 36 CFR 1234.32, reference (ai)).

C2.2.3.24. RMAs shall provide the capability for only authorized individuals to modify the metadata of stored records. However, RMAs shall not allow the editing of metadata fields that have been specifically identified in this Standard as not editable.

C2.2.3.25. RMAs shall enforce data integrity, referential integrity, and relational integrity.

C2.2.3.26. RMAs shall provide the capability to automatically synchronize multiple databases and repositories.

C2.2.4. Filing Electronic Mail Messages (E-mail).

C2.2.4.1. RMAs shall treat e-mail messages the same as any other record, and these shall be subject to all requirements of this Standard (see 32 CFR 1222.32 and 36 CFR 1234.24, references (aj) and (ak)).

C2.2.4.2. RMAs shall capture and automatically store the transmission and receipt data identified in Table C2.T4. if available from the e-mail system, as part of the record metadata when an e-mail message is filed as a record (see reference (ak)). RMAs shall not allow editing of Date and Time Sent or Date and Time Received. RMAs shall provide the capability for editing all other fields prior to filing. RMAs may map email transmission and receipt data to record metadata elements as described. Elements that are copied shall also be maintained separately to facilitate search, retrieval, transfer, and archival.

Table C2.T4. Transmission and Receipt Data

Transmission and Receipt Data	**E-mail Record Metadata Field Name**
The intelligent name[1] of the sender.	E-mail Sender, may be mapped to Author or Originator
The intelligent name of all primary addressees (or distribution lists).	E-mail Addressee, may be mapped to Addressee(s)
The intelligent name of all other addressees (or distribution lists).	E-mail Other Addressee, may be mapped to Other Addressee(s)
The date and time the message was sent.	E-mail Date Sent, may be copied as Publication Date
For messages received, the date and time the message was received (if available).	E-mail Date Received, may be mapped to Date Received
The subject of the message.	E-mail Subject may be mapped to Subject, and optionally as Title.

C2.2.4.3. RMAs shall provide user selectable options of filing e-mail and all its attachment(s) as a single record, filing selected e-mail item(s) as individual record(s), or to do both. When the attachment(s) is (are) filed as individual record(s), the user shall be provided the capability to enter the metadata required in table C2.T3. (see reference (ak)).

C2.2.4.4. RMAs shall not allow separate filing of Object Linking and Embedding (OLE) objects embedded in the body of the e-mail message.

C2.2.4.5. RMAs shall not require users to save attachments to their hard drive or other media prior to filing them separately from the e-mail message.

C2.2.4.6. RMAs shall automatically link e-mail records to their attachments when both are filed separately (see reference (ak)).

C2.2.4.7. RMAs shall provide graphical user interface capabilities that allow an authorized individual to map additional standard-compliant and/or Defense Messaging Service (DMS) e-mail application header fields to record metadata fields.

C2.2.5. <u>Filing records to be later transferred or accessioned to NARA</u>.

[1] Intelligent names are clear, uncoded, identifications of the individual.

C2.2.5.1. Additional metadata for records to be transferred or accessioned to NARA are identified in Table C2.T5. These are in addition to previously defined record metadata and are mandatory for data collection.

Table C2.T5. Record Metadata Components

Requirement	**Record Metadata Component**	**Reference/Comment**
Mandatory Data Collection		
	Scanned Records	
C2.T5.1.	Scanned Image Format and Version	NARA allows one of the following only; check with NARA (http://www.archives.gov/records-mgmt/initiatives/erm-products.html) for changes: TIFF 4.0 TIFF 5.0 TIFF 6.0 JPEG (all versions) GIF 87a GIF 89a ISO 12087-5 PNG 1.0
C2.T5.2.	Image Resolution	Image resolution relative to image encoding standard
	Portable Document Format (PDF) Records	
C2.T5.3.	Producing Application	Application used to render content to PDF
C2.T5.4.	Producing Application Version	
C2.T5.5	PDF Version	NARA allows versions 1.0 through 1.4 only; check with NARA for changes.
	Digital Photographs	
C2.T5.6	Caption	Narrative text describing each individual image in order to understand and retrieve it. Standard caption information typically includes the "who, what, when, where, why" about the photograph
	Web Records	
C2.T5.7	File Name	The file name of each web site file shall not exceed 99 ASCII characters, and with the path the name shall not exceed 254 ASCII characters.
C2.T5.8	Web Platform	Include the specific software applications and where available intended browser applications and versions
C2.T5.9	Web Site Name	Title of the website from the main entry page
C2.T5.10	Web Site URL	Include the filename of the starting page of the transferred content
C2.T5.11	Capture Method	Include name and description of harvester used. If PDF, include the software and version used to capture the PDF. If more than one clearly identify which content was captured by which method.
C2.T5.12	Capture Date	Date record was captured.

Table C2.T5. Record Metadata Components

Requirement	**Record Metadata Component**	**Reference/Comment**
C2.T5.13	Contact	Point of Contact information for person responsible for capturing the web record.
Mandatory Support		
	Scanned Records	
C2.T5.14	Image Bit Depth	Bit Depth relative to the image encoding standard.
	PDF Records	
C2.T5.15	Creating Application	Application used to create initial record content, includes version.
C2.T5.16	Document Security Settings	Additional Security added during PDF rendering.
	Digital Photographs	
C2.T5.17.	Photographer	Identify the full name (and rank, if military) and organization (agency, if Federal) of the photographer credited with the photograph, if available.
C2.T5.18.	Copyright	Indicate for each image whether there is a restriction on the use of that image because of a copyright or other intellectual property rights. Agencies must provide, if applicable, the owner of the copyright and any conditions on the use of the photograph(s), such as starting and ending dates of the restriction.
C2.T5.19.	Bit Depth	Identify the bit depth of the transferred files.
C2.T5.20.	Image Size	Specify the image height and width of each image in pixels.
C2.T5.21.	Image Source	Identify the original medium used to capture the images.
C2.T5.22.	Compression	Identify the file compression method used (if applicable) and the compression level (e.g., medium, high) selected for the image(s).
C2.T5.23.	ICCM/ICM profile	Provide custom or generic color profiles, if available, for the digital camera or scanner used [e.g., sRGB (standard Red Green Blue)].
C2.T5.24.	EXIF Information	If available, preserve and transfer to NARA the Exchangeable Image File Format (EXIF) information embedded in the header of image files (as TIFF tags or JPEG markers) by certain digital cameras (e.g., make and model of the digital camera).
	Web Records	
C2.T5.25	Content Management System	Application used to manage files on the web.

C2.2.5.2. RMAs shall provide an alert or warning that all PDF records to be transferred or accessioned to NARA must include embedded fonts, where applicable.

C2.2.6. Storing Records.

C2.2.6.1. RMAs shall provide at least one portal that provides access to all associated repositories and databases storing electronic records and their metadata. RMAs shall, through such a portal service or through an alternate service, provide metadata compliant with the DDMS (reference (c))

C2.2.6.2. The RMAs shall prevent unauthorized access to the repository(ies) (see 36 CFR 1222.50 and 44 U.S.C. 3105, references (y) and (al)).

C2.2.6.3. RMAs shall manage and preserve any record in any supported repository, regardless of its format, structure, or naming convention, so that, when retrieved, it can be reproduced, viewed, and manipulated in the same manner as the original. RMAs shall not require file extensions or associations to desktop applications as a condition to filing records (see references (y), (z), and (ac)).

C2.2.6.4. RMAs shall allow only authorized individuals to move or delete records from the repository (see 36 CFR 1222.50 and 36 CFR 1234.28, references (y) and (am)).

C2.2.6.5. RMAs shall raise an alert or notification if records have been removed from the repository outside of the RMA interface (see 36 CFR 1222.50 and 36 CFR 1234.28, references (y) and (am)).

C2.2.7. <u>Retention and Vital Records Management</u>.

C2.2.7.1. <u>Screening Records</u>.

C2.2.7.1.1. RMAs shall provide for sorting, viewing, saving, and printing list(s) of record folder metadata and/or record metadata regardless of media based on any combination of record category, disposition, folder and/or record metadata including user-defined metadata and system generated metadata.

C2.2.7.1.2. RMAs shall provide for sorting, viewing, saving, and printing life cycle information, eligibility dates, and events of user-selected record folders and records.

C2.2.7.1.3. RMAs shall allow the user to select and order the columns presented in the screening result list(s).

C2.2.7.1.4. RMAs shall provide authorized individuals with the capability to indicate when the specified event has occurred for records and record folders with event- and time-event-driven dispositions.

C2.2.7.1.5. RMAs shall provide for sorting, viewing, saving, and printing lists and partial lists of unscheduled record folders and/or records. These items have no approved final disposition but may be cutoff and subject to interim transfer.

C2.2.7.1.6. RMAs shall allow authorized individuals the capability to enter a reference "as-of" date to support screening of future lifecycle actions.

C2.2.7.2. Closing Record Folders.

C2.2.7.2.1. RMAs shall provide a capability for authorized individuals to close record folders to further filing after the specified event occurs.

C2.2.7.2.2. RMAs shall provide the capability only to authorized individuals to add records to a previously closed record folder and to reopen a previously closed record folder for additional public filing.

C2.2.7.3. Cutting Off Record Folders.

C2.2.7.3.1. RMAs shall be capable of implementing cutoff instructions for scheduled and unscheduled record folders. RMAs shall identify record folders eligible for cutoff, and present them only to the authorized individual for cutoff approval. Cutoff shall start the first disposition phase of a record or folder life cycle as controlled by the disposition instruction attached to the file plan record category or records schedule (see reference (z)).

C2.2.7.3.2. RMAs shall provide the capability to only authorized individuals to add records or make other alterations to record folders that have been cut off.

C2.2.7.4. Freezing/Unfreezing Records.

C2.2.7.4.1. RMAs shall provide the capability for only authorized individuals to extend or suspend (freeze) the retention period of record folders or records beyond their scheduled disposition (see 44 U.S.C. 2909 and 36 CFR 1228.54, references (an) and (ao)).

C2.2.7.4.2. RMAs shall provide a metadata element for authorized individuals to enter the reasons for freezing a record or record folder.

C2.2.7.4.3. RMAs shall identify record folders and/or records that have been frozen and provide authorized individuals with the capability to unfreeze them. Unless the records have been rescheduled in conjunction with the freeze, RMAs shall restore unfrozen records and/or record folders to the calculated phase of their lifecycle as if they were never frozen.

C2.2.7.4.4. RMAs shall allow authorized individuals to search, update, and view the reasons for freezing a record or record folder.

C2.2.7.5. Transferring Records.

C2.2.7.5.1. RMAs shall identify and present those record folders and records eligible for interim transfer and/or accession (see references (q) and (z)).

C2.2.7.5.2. RMAs shall, for records approved for interim transfer or accession and that are stored in the RMA's supported repository(ies), copy the pertinent records and associated metadata of the records and their folders to a user-specified filename, path, or device. For permanent records to be accessioned to the National Archives, the accessioning file(s) shall be made to conform to one of the formats and media specified in 36 CFR 1228.270[2] (see references (z), (ai), and (ap)). (See requirement C2.2.10.5.)

C2.2.7.5.3. RMAs shall, for records approved for accession and that are not stored in an RMA supported repository, copy the associated metadata for the records and their folders to a user-specified filename, path, or device. For permanent records to be accessioned to the National Archives, the metadata shall be made to conform to one of the formats and media specified in reference (ap).

C2.2.7.5.4. RMAs shall, for records approved for interim transfer or accession, provide the capability for only authorized individuals to delete the records and/or related metadata after successful transfer has been confirmed (see references (al) and (ao)). RMAs shall provide the capability to allow the organization to retain the metadata for records that were transferred or accessioned.

C2.2.7.5.5. RMAs shall provide documentation of transfer activities. This documentation shall be stored as records.

C.2.2.7.5.6. RMA shall provide the capability for bulk updating of the record’s and folder’s metadata as a result of the transfer action.

C2.2.7.5.7. RMAs shall, for records to be transferred or accessioned, comply with Chapter 5 herein.

C2.2.7.6. Destroying Records.

[2] If accessioning records and metadata to NARA in a format and media specified in 36 CFR 1228.270 causes a violation of the records' authenticity and/or integrity, the organization should contact NARA for guidance, see subparagraph C2.2.10.5.

C2.2.7.6.1. RMAs shall identify and present the record folders and records, including record metadata, that are eligible for destruction, as a result of reaching that phase in their life cycle. Records assigned more than one disposition must be retained and linked to the Record Folder (Category) with the longest retention period. Links to Record Folders (Categories) with shorter retention periods should be removed as they become due (see references (i), (z), and (ai)).

C2.2.7.6.2. RMAs shall, for records approved for destruction, present a second confirmation requiring authorized individuals to confirm the delete command, before the destruction operation is executed (see references (z) and (al)).

C2.2.7.6.3. RMAs shall delete electronic records approved for destruction in a manner such that the records cannot be physically reconstructed using commonly available file restoration utilities (see 36 CFR 1234.34, reference (aq)).

C2.2.7.6.4. RMAs shall provide an option allowing the organization to select whether to retain or delete the metadata of destroyed records.

C2.2.7.6.5. RMAs shall restrict the records destruction commands to authorized individuals (see references (y) and (al)).

C2.2.7.6.6. RMAs shall provide documentation of destruction activities. This documentation shall be stored as records.

C2.2.7.7. Cycling Vital Records.

C2.2.7.7.1. RMAs shall provide the capability for authorized individuals to enter the Vital Records Review and Update Cycle Period when creating or updating the file plan.

C2.2.7.7.2. RMAs shall provide the capability for authorized individuals to enter the date when the records associated with a vital records folder have been reviewed and updated.

C2.2.7.7.3. RMAs shall provide a means for identifying and aggregating vital records due for cycling.

C2.2.7.7.4. RMAs shall provide a means for identifying and aggregating vital records by previous cycle dates.

C2.2.7.7.5. RMAs shall provide a capability to allow an authorized individual to enter a reference “as-of” date to plan for future review cycles.

C2.2.7.8. Searching for and Retrieving Records.

C2.2.7.8.1. RMAs shall allow users to browse the records stored in the file plan based on their user access permissions.

C2.2.7.8.2. RMAs shall allow searches using any combination of the record category, record and/or folder metadata elements (see reference (c), reference (z)). This includes user-defined and system generated metadata.

C2.2.7.8.3. RMAs shall allow the user to specify partial matches and shall allow designation of "wild card" fields or characters.

C2.2.7.8.4. RMAs shall allow searches using combinations of Boolean and relational operators: "and," "and not," "or," "greater than" (>), "less than" (<), "equal to" (=),"not equal to" (<>), is blank, is null, not blank, and not null and provide a mechanism to override the default (standard) order of precedence.

C2.2.7.8.5. RMAs shall present the user a list of records and/or folders meeting the retrieval criteria, or notify the user if there are no records and/or folders meeting the retrieval criteria. RMAs shall allow the user to select and group results, and order the columns presented in the search results list for viewing, transmitting, printing, etc. (see reference (z)).

C2.2.7.8.6. RMAs shall provide to the user's workspace (filename, location, or path name specified by the user) copies of electronic records, selected from the list of records meeting the retrieval criteria, in the format in which they were provided to the RMA for filing (see reference (z)). RMAs shall not require that applications necessary to manipulate the records be installed on the retrieving workstation.

C2.2.7.8.7. RMAs shall provide the capability for filed e-mail records to be retrieved back into a compatible e-mail application for viewing, forwarding, replying, and any other action within the capability of the e-mail application.

C2.2.7.8.8. RMAs shall provide users a choice of retrieving filed records to their workspace or into a compatible application for viewing, editing, and any other action within the capability of the application.

C2.2.7.8.9. When the user selects a record for retrieval, RMAs shall present a list of available versions, defaulting to the latest version of the record for retrieval, but allow the user to select and retrieve any version.

C2.2.7.8.10. RMAs shall allow users to select any number of records, and their metadata, for retrieval from the search results list.

C2.2.7.8.11. RMAs shall allow the user to abort a search.

C2.2.8. Access Controls.

C2.2.8.1. Table C2.T6. summarizes requirements that refer to "authorized individuals" and offers additional information regarding example user-type roles and responsibilities. In general, Application Administrators are responsible for setting up the RMA infrastructure. Records Managers are responsible for records management administration. Privileged Users are those who are given special permissions to perform functions beyond those of typical users. RMAs shall provide the capability to allow organizations to define roles and responsibilities to fit their records management operating procedures.

Table C2.T6. Authorized Individual Requirements

Requirement	**Application Administrator**	**Records Manager**	**Privileged User**
C2.2.1.1. Create, edit, and delete file plan components and their identifiers.	Ensures that data structures are correctly installed and database links are in place	Enters file plan data	None
C2.2.1.2. Designate the metadata fields that are to be constrained to selection lists. Create and maintain selection lists for all supported data types for metadata items that are constrained to a pre-defined set of data..	Ensure database is correctly set up and installed	Define Lists	None
C2.2.1.3. Create, edit, and delete file plan metadata elements or attributes, and their associated selection lists..	Ensures that data structures are correctly installed and database links are in place	Enters file plan data	None
C2.2.1.4. Select where data collection for optional metadata fields is mandatory for a given organization.	Creates structures	Creates and Edits Fields	None
C2.2.1.5. Create, edit, and delete record folder components and their non-system generated identifiers.	Ensures that data structures are correctly installed and database links are in place	Enters file plan data	None
C2.2.1.6. Create, edit, and delete folder metadata elements or attributes, and their associated selection lists.	Ensures that data structures are correctly installed and database links are in place	As necessary	None
C2.2.1.7. Select where data collection for optional metadata fields is mandatory for a given organization.	Ensures that data structures are correctly installed and database links are in place	As necessary	None
C2.2.1.10. Allow to attach simple process actions to any or all metadata fields or to restrict record access based on the content of fields.	Creates rules and connects them to fields	Manually execute rules if necessary	None

Table C2.T6. Authorized Individual Requirements			
Requirement	**Application Administrator**	**Records Manager**	**Privileged User**
C2.2.2.1. Create, edit, and delete retention schedule components of record categories.	Ensures that data structures are correctly installed and database links are in place	Enters disposition data, enters event data, closes folders	Enters event data and closes folders
C2.2.2.4. Select cutoff as the trigger to begin final disposition calculations.	Ensures that data structure is correctly installed and database links are in place	Enters criteria and phase information	None
C2.2.2.6. Define the cutoff criteria and, for each life cycle phase, the following disposition components for a record category . . .	Ensures that data structure is correctly installed and database links are in place	Enters criteria and phase information	None
C2.2.2.8. Defining and naming disposition events.	As necessary	As necessary	As Necessary
C2.2.2.9. Enter an “as-of” reference date for lifecycle phase calculation.	As necessary	As necessary	None
C2.2.2.10. Change the disposition instructions.	None	Edits disposition information and manually executes rules necessary to reschedule	None
C2.2.3.3. Create, edit, and delete record metadata elements or attributes, and their associated pick lists.	Ensures that data structure is correctly installed and database links are in place	Creates Selection Lists	Enters data (all users)
C2.2.3.4. Select where data collection for optional metadata fields is mandatory for a given organization.	During setup	Advising	None
C2.2.3.12. Define and add user-defined metadata fields (e.g., project number, budget line) for site-specific requirements.	During setup	Advising	None
C2.2.3.14. Limit the record folders and record categories presented to a user or workgroup.	Record Categories during setup	Record Folders	Record Folders
C2.2.3.15. Limit the selection or pick list items presented to a user or workgroup.	During Set Up	As necessary	None
C2.2.3.16. Change a record folder or record category associated with a record.	As necessary	As necessary	None
C2.2.3.17. Change or delete links and associations.	Database is correctly installed and configured	Change links as necessary	None
C2.2.3.19. Remove links that affect disposition.	As necessary	As necessary	As necessary
C2.2.3.20. Define, update, and assign permissions for use of user-defined link types	During Set Up	As necessary	None
C2.2.3.24. Modify the metadata of stored records.	As necessary	Change data as necessary	Change data as necessary

Table C2.T6. Authorized Individual Requirements			
Requirement	**Application Administrator**	**Records Manager**	**Privileged User**
C2.2.4.7. Map additional standard-compliant and/or Defense Messaging Service (DMS) e-mail application header fields to record metadata fields.	During Set Up	As necessary	None
C2.2.6.4. Move or delete records from the repository.	As necessary	As necessary	None
C2.2.7.1.4. Indicate when the specified event has occurred for records and record folders with event and time-event driven dispositions.	Database setup	Link dispositions to record categories	Enter event information
C2.2.7.1.6. Enter a reference "as-of" date to support screening of future lifecycle actions.	As necessary	As necessary	None
C2.2.7.2.1. Close record folders to further filing after the specified event occurs.	As necessary	As necessary	As necessary
C2.2.7.2.2. Add records to a previously closed record folder or to reopen a previously closed record folder for additional public filing.	As necessary	As necessary	As necessary
C2.2.7.3.1. Approve cutoff.	As necessary	Routine work	None
C2.2.7.3.2. Add records or make other alterations to record folders that have been cut off.	Database support	Enters limits	None
C2.2.7.4.1. Extend or suspend (freeze) the retention period of record folders or records beyond their scheduled disposition.	Database and business rules	Freezing/ Unfreezing	None
C2.2.7.4.2. Enter the reasons for freezing a record or record folder.	Database and business rules	Freezing/ Unfreezing	None
C2.2.7.4.3. Unfreeze capability.	Database and business rules	Freezing/ Unfreezing	None
C2.2.7.4.4. Search, update, and view the reasons for freezing a record or record folder.	Database and business rules	Freezing/ Unfreezing	None
C2.2.7.5.4. Delete the records and/or related metadata after successful transfer has been confirmed.	As necessary	As necessary	None
C2.2.7.6.2. Confirm the delete command, before the destruction operation is executed.	As necessary	As necessary	None
C2.2.7.6.5. Access to records destruction commands.	As necessary	As necessary	None
C2.2.7.7.1. Enter the Vital Records Review and Update Cycle Period when creating or updating the file plan.	Ensure database structure is adequate and correctly installed	Enters cycling data	None
C2.2.7.7.2. RMAs shall provide the capability for authorized individuals to enter the date when the records associated with a vital records folder have been reviewed and updated.	Ensure database structure is adequate and correctly installed	Enters cycling data	Cycles and Updates Records
C2.2.7.7.5. Enter a reference "as-of" date to plan for future review cycles.	As necessary	As necessary	As Necessary

Table C2.T6. Authorized Individual Requirements

Requirement	**Application Administrator**	**Records Manager**	**Privileged User**
C2.2.8.1. Edit the roles defined in this standard and to create and maintain user- defined roles.	As necessary	As necessary	None
C2.2.8.3. Allow access to the RMA.	As necessary	As necessary	None
C2.2.8.3.2. Define the minimum length of the Password field.	Define minimum length	None	None
C2.2.9.2. Determine which of the objects and specified actions listed in subparagraph C2.2.9.1. are audited.	Manage audits	None	None
C2.2.9.3. Set up specialized reports to:	Create reports	None	None
C2.2.9.5. Export and/or backup and remove audit files from the system.	Export and/or backup and remove audit files	File audit logs as records	None
C2.2.10.3 Map producing system standard and user-defined metadata to RMA standard or user-defined metadata fields.	Database Setup	During Export/Import	None

C2.2.8.2. RMAs shall provide a graphical user interface capability to authorized individuals to edit the roles defined in this standard and to create and maintain user- defined roles.

C2.2.8.3. Upon installation, RMAs shall require the default password for the super user or application administrator be changed from the default.

C2.2.8.4. The RMA, in conjunction with its operating environment, shall use identification and authentication measures that allow only authorized individuals access to the RMA. At a minimum, the RMA will implement identification and authentication measures that require the following (see EO 12958, and EO 12968, references (d) and (ar)).

C2.2.8.4.1. Userid.

C2.2.8.4.2. Password. (RMAs shall provide the capability for authorized individuals to define the minimum length of the Password field.)

C2.2.8.4.3. Alternative methods, such as Biometrics, Common Access Cards (CAC), or Public Key Infrastructure (PKI), in lieu of or in conjunction with the above, are acceptable. If used in lieu of, the alternative must provide at least as much security.

C2.2.8.5. RMAs shall provide the capability for only individuals with Application Administrator access to authorize access capabilities to any combination of the items identified in Table C2.T5. to individuals and to groups.

C2.2.8.6. RMAs shall provide the capability to define different groups of users with different access privileges. RMAs shall control access to file plan components, record folders, and records based on group membership as well as user account information. At a minimum, access shall be restricted to appropriate portions of the file plan for purposes of filing and/or searching/retrieving (see references (z) and (am)).

C2.2.8.7. RMAs shall provide a web user interface, as a minimum, for filing, and search and retrieval of records. This shall provide a minimum of 128-bit encryption and be PKI-enabled, as well as provide all the mandatory access controls.

C2.2.8.8. RMAs shall support simultaneous multiple-user access to all components of the RMA, the metadata, and the records.

C2.2.9. System Audits.

C2.2.9.1. The RMA, in conjunction with its operating environment, shall provide an audit capability to log the actions, date, time, unique object identifier(s) and user identifier(s) for actions performed on the following RMA objects at a minimum:

C2.2.9.1.1. User Accounts.

C2.2.9.1.2. User Groups.

C2.2.9.1.3. Records and Record Folders.

C2.2.9.1.4. Associated metadata elements.

C2.2.9.1.5. File plan components.

C2.2.9.2. These actions include retrieving, creating, deleting, searching, and editing actions (see reference (d)). The RMA shall provide a capability whereby only authorized individuals can determine which of the objects and specified actions listed in subparagraph C2.2.9.1. are audited (see reference (d)).

C2.2.9.3. The RMA, in conjunction with its operating environment, shall provide audit analysis functionality whereby an authorized individual can set up specialized reports to:

C2.2.9.3.1. Determine what level of access a user has and to track a user’s actions over a specified time period. These are the specified actions listed in subparagraph C2.2.9.1 (see references (d) and (z)).

C2.2.9.3.2. Facilitate reconstruction, review, and examination of the events surrounding or leading to mishandling of records, possible compromise of sensitive information, or denial of service.

C2.2.9.4. RMAs shall provide the capability to file the audit data as a record (see reference (z)).

C2.2.9.5. The RMA, in conjunction with its operating environment, shall allow only authorized individuals to export and/or backup and remove audit files from the system.

C2.2.9.6. The RMA, in conjunction with its operating environment, shall not allow audit logs to be edited.

C2.2.10. Product Combinations. Product combinations, that are the result of integrating two or more distinct products, where typically, one product primarily creates records and another product performs the records' retention schedule tracking, shall meet the following requirements. For clarity the product that creates records will be referred to as producing systems throughout this standard.

C2.2.10.1. Preventing Naming Conflicts. If producing system maintains metadata with a name specified by this standard, the content and context of the metadata shall meet the content and context criteria of this standard.

C2.2.10.2. Metadata Mapping Defaults. Producing system metadata with names specified in this standard shall be mapped to like named metadata in the RMA by default.

C2.2.10.3. Metadata Mapping Management. Product combinations shall provide a graphical user interface capability for an authorized individual to map producing system standard and user-defined metadata to RMA standard or user-defined metadata fields.

C2.2.10.4. Data Collection Management. Product combinations shall manage metadata such that users will enter information only one time per record.

C2.2.10.5. Metadata Synchronization and Integrity. If metadata is kept in multiple locations, product combinations shall ensure metadata is synchronized across all locations within five minutes of being changed in any location.

C2.2.10.6. Filing Support. Product combinations shall provide a single user interface that supports all filing operations including establishing links and/or references among records.

C2.2.10.7. Search and Retrieval. Product combinations shall allow users to search and retrieve records from the same interface they filed them. (e.g. The user will not have to open a stand alone records application interface to search for records if that user was able to file from a producing system.)

C2.2.10.8. Permissions Management. Product combinations shall automatically incorporate or coordinate user permissions in the RMA component with the producing system. The permissions in the RMA component shall take precedence for all records.

C2.2.10.9. Permissions Synchronization. Product combinations shall synchronize user permissions among the components of the product combination when multiple copies of the permissions are maintained.

C2.2.11. System Management Requirements. The following functions are typically provided by the operating system or by a database management system. These functions are also considered requirements to ensure the integrity and protection of organizational records. They shall be implemented as part of the overall records management system even though they may be performed externally to an RMA.

C2.2.11.1. Backup of Stored Records. The RMA system shall provide the capability to automatically create backup or redundant copies of the records and their metadata (see references (z), (ah) and (am)). The RMA backup capability shall ensure synchronization between all record category, file plan, folder, record metadata and content repositories.

C2.2.11.2. Storage of Backup Copies. The method used to back up RMA database files shall provide copies of the records and their metadata that can be stored off-line and at separate location(s) to safeguard against loss due to system failure, operator error, natural disaster, or willful destruction (see 36 CFR 1234.30, reference (as)).

C2.2.11.3. Recovery/Rollback Capability. Following any system failure, the backup and recovery procedures provided by the system shall:

C2.2.11.3.1. Ensure data integrity by providing the capability to compile updates (records, metadata, and any other information required to access the records) to RMAs.

C2.2.11.3.2. Ensure these updates are reflected in RMA files, and ensuring that any partial updates to RMA files are separately identified. Also, any user whose updates are incompletely recovered, shall, upon next use of the application, be notified that a recovery has been attempted. RMAs shall also provide the option to continue processing using all in-progress data not reflected in RMA files (see references (z) and (am)).

C2.2.11.4. Rebuild Capability. The system shall provide the capability to rebuild from any backup copy, using the backup copy and all subsequent system audit trails (see reference (z)).

C2.2.11.5. Storage Availability and Monitoring. The system shall provide for the monitoring of available storage space. The storage statistics shall provide a detailed accounting of the amount of storage consumed by RMA processes, data, and records. The system shall notify individuals of the need for corrective action in the event of critically low storage space (see reference (z)).

C2.2.11.6. Safeguarding. The RMA, in conjunction with its operating environment, shall have the capability to activate a keyboard lockout feature and a screen-blanking feature (see reference (d)).

C2.2.12. Additional Baseline Requirements. The following are records management requirements that shall be implemented by the organization, but not necessarily by the RMAs.

C2.2.12.1. Electronic Calendars and Task Lists. Some electronic systems provide calendars and task lists for users. These may meet NARA's definition of a record (see reference (k)). Calendars and task lists that meet the definition of records shall be managed as any other record. If the RMA being acquired does not have the capability to extract calendars and task lists from the software application that generates them, the user organization shall implement processes or procedures to enable those records to be managed by the RMA.

C2.2.12.2. External E-mail. Some organizations use separate e-mail systems for Internet e-mail or other wide area network e-mail. These records shall be handled as any other e-mail records. If the RMA being acquired does not provide the capabilities specified in paragraph C2.2.3, the user organization shall implement processes or procedures to enable these records to be managed by the RMA (see reference (ak)).

C2.2.12.3. Ability to Read and Process Records. Since RMAs are prohibited (see subparagraph C2.2.3.8.) from altering the format of stored records, the organization shall ensure that it has the ability to view, copy, print, and, if appropriate, process any record stored in RMAs for as long as that record must be retained. The organization may meet this requirement by:

C2.2.12.3.1. Maintaining the hardware and software used to create or capture the record.

C2.2.12.3.2. Maintaining hardware and software capable of viewing the record in its native format.

C2.2.12.3.3. Ensuring backward compatibility when hardware and software is updated, or:

C2.2.12.3.4. Migrating the record to a new format before the old format becomes obsolete. Any migration shall be pre-planned and controlled to ensure continued reliability of the record (see reference (as)).

C2.2.12.4. Distribution Lists. If the RMA is unable to access and store e-mail distribution lists from the e-mail server, the organization shall implement procedures to extract and store them as records.

C2.2.12.5. Accessioning Records to NARA. When accessioning records and metadata to NARA, if conforming to formats and media specified in 36 CFR 1228.270 (reference (ap)) causes a violation of the records' authenticity and/or integrity, the organization shall contact NARA for guidance.

C2.2.12.6. Applying Records Retention Schedule to Backup Copies. The using organization shall schedule the backup copies and recycle or destroy the medium in accordance with the retention schedule.

C3. CHAPTER 3

MANAGEMENT OF CLASSIFIED RECORDS

C3.1. MANAGEMENT OF CLASSIFIED RECORDS

C3.1.1. The following requirements address the management of classified records. As such, these requirements are only mandatory for those RMAs that manage classified records. These requirements are in addition to those requirements outlined in Chapter 2. In this chapter, the word "shall" identifies mandatory system standards for vendors who support the management of classified records. The word "should" identifies design objectives that are desirable but not mandatory for supporting classified records management. Additionally, requirements for safeguarding and providing security for classified records are not in the scope of this document, since they are provided in other more applicable directives and regulations.

C3.1.2. Mandatory Metadata Fields for Classified Records. RMAs shall provide a capability by which a user can add metadata that describes a classified record. These metadata elements are shown in Table C3.T1. (see EO 12958, as amended by EO 13292 and 32 CFR 2001, references (d) and (at)). Mandatory Data Collection indicates that RMAs shall ensure population of the associated data structure with non-null values. Conditional Data Collection indicates that the RMA shall check values in interdependent fields and require population as described. Mandatory Data Support indicates that the RMA shall provide a capability to support creating and managing the metadata. Where data collection is not mandatory, RMAs shall behave in a predictable manner as a result of queries or other operations when the fields are not populated.

Table C3.T1. Classified Record Components

Requirement	**Classified Record Component**	**Reference/ Comment**
Mandatory Data Collection		
C3.T1.1.	Initial Classification	EO 12958 Sec. 1.2 and Sec 1.6a(1); and 32 CFR 2001.21 (b), (references (d) and (at)). The Option List must include only the following: Confidential Secret Top Secret Unclassified
C3.T1.2.	Current Classification	EO 12958 Sec. 1.2 and Sec. 1.6a(1); and 32 CFR 2001.21 (b), (references (d) and (at)). The Option List must include only the following: Confidential Secret Top Secret Unclassified
Conditional Data Collection		
C3.T1.3.	Reason(s) For Classification	EO 12958 Sec. 1.4 and Sec. 1.6a(5); and 32 CFR

Table C3.T1. Classified Record Components		
Requirement	**Classified Record Component**	**Reference/ Comment**
		2001.21 (a)(3), 2001.22(c), and DoD 5200.1R (references (d), (at), and (ah), respectively). Mandatory only when "Classified By" is not blank or null
C3.T1.4.	Classified By (also called classification authority)	EO 12958 Sec. 1.3 and Sec. 1.6a(2); and 32 CFR 2001.21(a)(1) (references (d) and (at)). Mandatory if Derived From field is blank or null.
C3.T1.7.	Classifying Agency	
C3.T1.5.	Derived From	EO 12958 Sec. 2.1 and 2.2; and 32 CFR 2001.22(a)(2) and (b) (references (d) and (at)). Mandatory if Classified By field is blank or null.
C3.T1.6.	Declassify On	EO 12958 Sec. 1.5, Sec. 1.6(a)(4); and 32 CFR 2001.21(a)(4), (d), and (e) and 2001.22(d) (references (d) and (at)). Mandatory for all but restricted data or formerly restricted data. The declassify trigger be a date, an event, an exemption category and date, or a combination of dates or events.
Mandatory Data Support		
C3.T1.8.	Downgrade On	EO 12958 Sec. 6.1(p), 32 CFR 2001.32 (b) (4)(ii) (reference (d), (at), (ah)). The downgrade trigger can be a date, an event, or a combination of dates or events.
C3.T1.9.	Downgrade Instructions	Mandatory if Downgrade On is populated
C3.T1.10.	Reviewed On	EO 12958 Sec. 3.4 and Sec. 3.5 and 32 CFR 2001.31 and 2001.33 (references (d) and (at))
C3.T1.11.	Reviewed By	Mandatory if Reviewed On is populated.
C3.T1.12.	Downgraded On	32 CFR 2001.24 (reference (at))
C3.T1.13.	Downgraded By	Mandatory if Downgrade On is populated.
C3.T1.14.	Declassified On	EO 12958, Part 3 and 32 CFR 2001.24 (references (d) and (at))
C3.T1.15.	Declassified By	Mandatory if Declassified On is populated.
C3.T1.16.	Upgraded On	
C3.T1.17.	Reason(s) for Upgrade	Mandatory if Upgraded On is populated
C3.T1.18.	Upgraded By	Mandatory if Upgraded On is populated

C3.1.3. Initial Classification. RMAs shall provide a capability by which a user can select and/or edit the Initial Classification prior to filing.

C3.1.4. Current Classification. RMAs shall provide a capability by which a user can select and/or edit the Current Classification prior to filing.

C3.1.5. Originally Classified Records. RMAs shall require that when the "Derived From" field is not completed, the "Classified By" and "Reason(s) for Classification" fields must be completed (see EO 12958, part I, section 1.7, reference (d)).

C3.1.6. Derivatively Classified Records. RMAs shall provide one or more fields to indicate when records have been derivatively classified. These fields shall support entering one or more of the following:

C3.1.6.1. “Multiple Sources” or

C3.1.6.2. Title(s) of classification guide(s), or

C3.1.6.3. The title, publication date, and originating organization of the source document(s) (see 32 CFR 2001.22, reference (at)).

C3.1.7. Multiple Derivative Sources. When the user enters "Multiple Sources" in the “Derived From” fields, RMAs shall provide the capability to enter the title, date, and originating organization for each source (see EO 12958, Section 2.2 (b) and 32 CFR 2001.22, references (d) and (at)).

C3.1.8. Declassify On Event. When "Event" is selected in the "Declassify On" field, the RMA shall prompt the user to enter text that describes the declassification event.

C3.1.9. Declassify On Time Frame. When a date is inserted in the "Declassify On" field, RMAs shall verify that the date is no more than the mandated period of time from the Publication Date. If that time frame is exceeded, an alert shall be presented to the user. (See EO 12958, Section 1.6 (4), reference (d)).

C3.1.10. Maintaining the Declassify On Time Frame. RMAs shall provide the capability for authorized individuals to establish and maintain the period of time used to verify the dates in the "Declassify On" fields, both to make the classification period more restrictive or to accommodate changes to the mandatory classification period (see EO 12958, Section 1.6 (4), reference (d)).

C3.1.10.1. Updating Declassify On when Time Frame is updated. Upon request of an authorized individual, the RMA shall automatically calculate a new declassify on date for all records that were marked with the automatic declassification date. (These are records that had a declassify date calculated from the declassify on time frame.) RMAs shall not change declassify on dates that were not automatically calculated.

C3.1.11. Storing Declassified Records. RMAs shall provide a capability to automatically transfer and expunge declassified records from the classified repository upon direction by an authorized individual or set up during initial configuration. The RMA shall allow the authorized individual to indicate whether the record metadata and history shall be retained annotated with the new location of the declassified record, in an unclassified repository.

C3.1.12. Classification Guides. RMAs shall provide a capability that allows an authorized individual to input and manage multiple classification guides. Each guide record or object shall include the title, date, and originating organization, which will be populated into an appropriate “Derived From” field when a user selects a guide (see reference (at)). RMAs shall provide the capability to allow the user to select topics from one or more classification guides.

C3.1.13. Mapping Classification Guide Fields. RMAs shall provide a capability to allow only an authorized individual to map the fields of a classification guide to the record metadata fields that they should automatically populate, when a user selects a topic. By default, the RMA shall automatically populate the following fields, which shall be editable prior to filing:

C3.1.13.1. Initial and Current Classification (if available from the guide).

C3.1.13.2. Supplemental Markings (if available from the guide) (see 32 CFR 2001.15 (b)(7), reference (at)).

C3.1.13.3. Declassify On (if available from the guide).

C3.1.14. Confirming Accuracy Prior to Filing. RMAs shall provide the capability to confirm the accuracy of all user editable metadata items prior to filing.

C3.1.15. Editing Records. RMAs shall allow only authorized individuals to edit metadata items after a record has been filed.

C3.1.16. Current Classification. When the entry in the "Current Classification" field is changed, RMAs shall ensure that the "Upgraded On," "Downgraded On," or "Declassified On" field, whichever is appropriate, is populated with an appropriate date (see EO 12958, Part 3, reference (d)).

C3.1.17. Exemption Categories. RMAs shall provide the capability for an authorized individual to enter or update exemption category(ies) in the "Declassify On" field and optionally enter a declassify on date or event that surpasses the declassify on timeframe (see EO 12958, Section 3.4 (b) and 32 CFR 2001.21 (e), references (d) and (at)).

C3.1.18. Record History Audit. The RMA shall capture and link an audit history of each record by capturing the replaced metadata value and the identity of the person who entered that value, and appending them to a record audit history file. The metadata fields to be captured shall be authorized individual selectable. The record history audit shall be included with the other record metadata when transferring or accessioning records (see EO 12958, Part 3 and 32 CFR 2001.21, Subpart E, see references (d) and (at)).

C3.1.19. Using the Record History Audit. The RMA shall provide the capability to view, copy, save, and print the record history audit based on user permissions; shall not allow the editing of the record history audit; and shall provide the capability for only authorized individuals to delete the record history audit if it has been filed as record.

C3.1.20. Marking Search and Screening Results Lists Printouts and Displays. Current Classification shall always be the leftmost column in any results list and shall not be movable (see 32 CFR 2001.20, reference (at)).

C3.1.21. Access Conflicts. The RMA, in conjunction with its operating environment, shall ensure that if there is a conflict between the individual's access criteria and the access criteria of the group(s) assigned, the individual's access criteria shall take precedence (see EO 12958, Part 4, reference (d)).

C3.1.22. Searching Classified Records. RMAs shall provide a mechanism whereby users can search for records based on metadata contained in Table C3.T1.

C3.1.23. Restricting Access. The RMA shall provide a capability whereby authorized individuals may restrict access to records and their metadata based on access criteria. In addition to baseline access restriction capabilities, these additional criteria include (see EO 12958, Part 4, reference (d)).

C3.1.23.1. Current Classification (see subparagraph C3.T1.2.).

C3.1.23.2. Supplemental Marking List (see subparagraph C2.T2.6.).

C3.1.23.3. Metadata Elements identified by the organization to be used for access control.

C3.1.24. Access Control. Table C3.T2. summarizes requirements that refer to "authorized individuals" and offers additional information regarding user-type responsibilities. In general, Application Administrators are responsible for setting up the RMA infrastructure. Records Managers are responsible for records management administration. Privileged Users are those who are given special permissions to perform functions beyond those of typical users.

Table C3.T2. Authorized Individual Requirements			
Requirement	**Application Administrator**	**Records Manager**	**Privileged User**
C3.1.9. Maintaining the Declassify On Time Frame. …establish and maintain the period of time used to verify the dates in the "Declassify On" fields,	Database installed and properly set up. Enter and maintain data.	None	None
C3.1.9.1. Updating Declassify On when Time Frame is updated. Upon request of a authorized individual, the RMA shall automatically calculate a new declassify on date ….	None	Request	Request
C3.1.10. Storing Declassified Records. … automatically transfer and expunge declassified records from the classified repository upon direction by an authorized individual or set up during initial configuration. … indicate whether the record metadata and history shall be retained annotated with the new location of the declassified record, in an unclassified repository.	During Setup	Direction	None
C3.1.11. Classification Guides. … input and manage multiple classification guides. … select topics from one or more classification guides.	Database installed and properly set up	None	Enter and maintain data (Security person)
C3.1.12. … map the fields of a classification guide to the record metadata fields …:	Database installed and properly set up	Map	None
C3.1.14. … edit metadata items after a record has been filed.	As necessary	As necessary	As necessary (downgrading and reclassification, etc.)
C3.1.16. Enter or update exemption category(ies) in the "Declassify On" field.	Database installed and properly set up	None	Enter and maintain data (Security person)
C3.1.17. Select which metadata fields to capture.	As necessary	As necessary	None
C3.1.18. Delete the record history audit after filing as a record.	As necessary	As necessary	None
C3.1.22. … restrict access to records and their metadata based on access criteria	User accounts, Access Control Lists and Database properly set up	None	None
C3.2.1. (Optional) Determine which metadata fields require classification for a given organization.	Database and business rules properly defined, installed and set up	None	None

C3.1.25. Classified National Security Information Not Declared as Records.

C3.1.25.1. Software applications handling working papers that contain classified national security information shall provide the capability for metadata to be entered and linked to the document as follows:

C3.1.25.1.1. Working Paper Indicator.

C3.1.25.1.2. Security Classification Level/Current Classification.

C3.1.25.1.3. Title.

C3.1.25.1.4. Creation Date.

C3.1.25.1.5. Creator.

C3.1.25.2. Software applications handling working papers that contain classified national security information shall provide the capability for users to search on the working paper indicator. The search metadata should be compliant with the DDMS (reference (c)).

C3.1.25.3. Software applications handling classified national security information that do not qualify as working papers, even if not declared as records, shall satisfy all the mandatory requirements of Chapter 3 of this standard.

C3.1.25.4. Software applications shall provide the capability for user-selected working papers to satisfy paragraph C3.1.22.3.

C3.1.25.5. Software applications shall satisfy paragraph C3.1.21 for all classified national security information.

C3.2. <u>OPTIONAL SECURITY FEATURES</u>

C3.2.1. <u>Field-level Classification</u>. RMAs should provide the capability to allow authorized individual-selected metadata fields to be provided their own classification.

C3.2.2. <u>Marking Printouts and Displays</u>. Current classification, reasons for classification, and downgrading instructions should be required metadata items for displays, printouts, reports, queries, review lists, etc. when organizations implement classification restrictions on individual-selected metadata fields. The highest classification level shall be displayed (in the header and footer of the printout) when aggregate results are displayed (see 32 CFR 2001.20, reference (at)).

C3.2.3. Redacted Version Notification. Where appropriate, RMAs should have the capability to inform the user that a redacted version is available in an open repository.

C3.2.4. Populating "Reasons for Classification" from the Guide. RMAs should provide the capability for the “Reasons for Classification” to be appropriately automatically populated (if available) when a topic from a classification guide is selected.

C3.2.5. Tracking Recipients of Classified Records. RMAs should provide capabilities to assist organizations in tracking recipients or holders of classified information sent from or copied out of the RMA (see 32 CFR 2001.13, reference (at)).

C3.3. PRODUCT COMBINATIONS

C3.3.1. RMAs should interact with auto-classifiers, tools for downgrading and declassifying, and other tools that support the creation of classified records. These tools should automatically pass record metadata from the creating environment to the appropriate RMA record metadata fields to minimize data entry by the user.

(This page intentionally left blank.)

C4. CHAPTER 4

MANAGING RECORDS FOR THE PRIVACY ACT AND THE FREEDOM OF INFORMATION ACT

C4.1. MANAGEMENT OF PRIVACY ACT RECORDS

C4.1.1. The following requirements address RMAs that support managing records stored in systems of records (SORs). As such, these requirements are mandatory for only those RMAs that host SORs. Organizational compliance with Privacy Act may be implemented outside the scope of an RMA. These requirements are in addition to those requirements outlined in Chapters 2 and 3. In this chapter, the word "shall" identifies mandatory system standards for managing SOR records. The word "should" identifies design objectives that are desirable but not mandatory. Additionally, requirements for safeguarding and providing security for SOR records are not in the scope of this document, since they are provided in other more applicable directives and regulations.

C4.1.2. System of Records Notifications. RMAs shall provide functionality that supports authorized personnel in preparing and posting System of Records Notices (SORNs) to the Federal Register.

C4.1.2.1. System of Record Notice Metadata. At a minimum the RMA shall link the following SORN metadata to the SORN record (see 5 U.S.C. 552a (e)(4), and DoD 5400.11-R (C6.3), references (au) and (av)).

Table C4.T1. System of Record Components

Requirement	**System of Record Component**	**Reference/ Comment**
Mandatory Data Collection		
	Notice Record	
C4.T1.1.	System Identification	5 U.S.C. 552a (e)(4a), and DoD 5400.11-R (C6.3, C6.3.1.1.1, C6.3.2), references (au) and (av). Limited to 21 alphanumeric characters for DoD systems.
C4.T1.2.	System Name	5 U.S.C. 552a (e)(4a) and DoD 5400.11-R (C6.3, C6.3.1.1.2, C6.3.3), references (au) and (av). Limited to 55 alphanumeric characters for DoD systems
C4.T1.3.	Responsible Official	5 U.S.C. 552a (e)(4f) and DoD 5400.11-R (C6.3, C6.3.1.1.10, C6.3.10), references (au) and (av). Title and business address of responsible agency official.
C4.T1.4.	System Location	5 U.S.C. 552a (e)(4a) and DoD 5400.11-R (C6.3, C6.3.1.1.3, C6.3.4), references (au) and (av). Addresses (repeating field) of each location where

Table C4.T1. System of Record Components		
Requirement	**System of Record Component**	**Reference/ Comment**
		the system or segment of the system is maintained. Classified addresses are not listed, but the fact that they are classified is indicated.
C4.T1.5.	Category of Individuals	5 U.S.C. 552a (e)(4b) and DoD 5400.11-R (C6.3, C6.3.1.1.5, C6.3.5), references (au) and (av). Discussion that includes an estimated number and specific categories of individuals to whom records pertain.
C4.T1.6.	Category of Records	5 U.S.C. 552a (e)(4b) and DoD 5400.11-R (C6.3, C6.3.1.1.5, C6.3.6), references (au) and (av). Clear description of the types of records maintained in the system.
C4.T1.7.	Authority	DoD 5400.11-R (C6.3, C6.3.1.1.6, C6.3.7) USC Title 5, 552a. (e)(3a), references (au) and (av). Links to authority records. Could be a repeating field
C4.T1.8.	Routine Uses	DoD 5400.11-R (C6.3, C6.3.1.1.8, C6.3.9) USC Title 5, 552a. (e)(3a) , references (au) and (av). Information for how the information will be used. Blanket uses include one or more of; Law Enforcement, Disclosure when Requesting Information, Congressional Inquiries, Private Relief Legislation, Disclosure Required by International Agreements, Disclosure to Stat and Local Taxing Authorities, and Disclosure to the Office of Personnel Management. This list may be supplemented by specific routine use information.
C4.T1.9.	Rules	5 U.S.C. 552a (e)(4e, f, g, h), and DoD 5400.11-R (C6.3, C6.3.1.1.12, C6.3.22) references (au) and (av). The name of the documentation providing the access rules for this SOR
	Administrative Data	
C4.T1.10.	NID	The unique identifier for this notification
C4.T1.11.	NType	One of: Initial, Amending, Standdown.
C4.T1.12.	NPosting	Indicates the date and volume of the federal register or the date and name of publication prepared for the appropriate congressional committee recipient.
C4.T1.13.	NDate	The date this notification was published in the federal register.
C4.T1.14.	NComments	Any comments documenting unique circumstances of this notification
C4.T1.15.	Preparer	The author or preparer of this SORN
	ReleasedBy	The name of the person responsible for ensuring publication of the SORN

Table C4.T1. System of Record Components		
Requirement	**System of Record Component**	**Reference/ Comment**
Conditional Data Collection		
C4.T1.16.	Purpose of System	5 U.S.C. 552a (e)(3a) and DoD 5400.11-R (C6.3, C6.3.1.1.7, C6.3.8), references (au) and (av). Discussion of the system purpose. Mandatory for new system
C4.T1.17.	Nature of Last Change	Discussion of the changes to the purpose and/or use of the system. Includes deactivation. Mandatory for altered systems.
C4.T1.18.	Exemptions	5 U.S.C. 552a (j, k) and DoD 5400.11-R (C6.3, C6.3.1.1.15, C6.3.15), references (au) and (av). May be blanket exemption(s) under Section J(2) of the Privacy Act of 1974 or one or more specific exemption(s) under Section K (1-7) of the same. Classified materials are covered by a blanket exemption under Section K (1) of the Privacy Act of 1974. Mandatory if exemptions apply.
C3.T1.19.	Matching Programs	Links to matching program records or descriptions. Mandatory if SOR participates in one or more matching program.
Mandatory Data Structure		
C4.T1.20.	Notices	5 U.S.C. 552a (e)(4) and DoD 5400.11-R (C6.3, C6.3.1.1.11, C6.3.11), references (au) and (av). Link to/from notices about this SOR.
C4.T1.21.	Information Collection	Identify or link to the form(s) used to collect the personal information stored in this system of records.
C4.T1.22.	Failure to Provide Notice	5 U.S.C. 552a (e)(3a), reference (au). Notice of possible adverse actions that may be taken if the individual fails to provide requested personal information.
Mandatory Support		
C4.T1.23.	User-defined Fields	

C4.1.2.2. System of Record Notice Preparation. The RMA shall provide interfaces with common office applications or document management systems to support the drafting of the SORN and rules documents. The RMA shall collect pertinent metadata from the office application or document management system file properties/metadata to pre-populate metadata elements to the degree possible (see 5 U.S.C. 552a (e)(4) and DoD 5400.11-R (C6.3), references (au) and (av)).

C4.1.3. Privacy Case Files. RMAs shall provide authorized individuals the capability to create and manage Privacy Case Files (see DoD 5400.11-R (C3.3.16), reference (av)).

C4.1.3.1. Privacy Case File Metadata. At a minimum the RMA shall capture the following Privacy Act file metadata (see DoD 5400.11-R (C3.3.16), reference (av)).

Table C4.T2. Privacy Act File Components

Requirement	**Privacy Act File Component**	**Reference/ Comment**
Mandatory Data Collection		
C4.T2.1.	FileID	5 U.S.C. 552a (e)(4a) and DoD 5400.11-R (C6.3, C6.3.1.1.1, C6.3.2), references (au) and (av). Limited to 21 alphanumeric characters for DoD systems.
C4.T2.2.	FileName	5 U.S.C. 552a (e)(4a) and DoD 5400.11-R (C6.3, C6.3.1.1.2, C6.3.3), references (au) and (av). Limited to 55 alphanumeric characters for DoD systems
Mandatory Support		
C4.T2.3.	User-defined Fields	

C4.1.3.2. Privacy Case File Links. RMAs shall link to or copy into Privacy Case files the following:

C4.1.3.2.1. Requests for Amendment or Access

C4.1.3.2.2. Access Grant or Denial Records

C4.1.3.2.3. Appeals Records

C4.1.3.2.4. Appeal Response Records

C4.1.3.2.5. Amended Records

C4.1.3.2.6. Disputes/Statements of Disagreement

C4.1.3.2.7. Correspondence and Coordination Records relating to any of the above

C4.1.4. Individual Access Requests. RMAs shall provide functionality that supports authorized personnel in recording, tracking and managing a request from a private individual (see 5 U.S.C. 552a (d) and DoD 5400.11-R (C3.1), references (au) and (av)).

C4.1.4.1. Individual Access Request (IAR) Metadata. At a minimum the RMA shall support gathering the following IAR metadata and store and manage the request as a record (see DoD 5400.11-R (C3.1), reference (av)).

Table C4.T3. Individual Access Request Components

Requirement	**Individual Access Component**	**Reference/ Comment**
Mandatory Data Collection		
C4.T3.1.	Request ID	Unique identifier for this request
C4.T3.2.	Request Author	Identification and contact information for person requesting information
C4.T3.3	Nature of Request	One of Review, Dispute, or Disclosure Accounting
C4.T3.4	Details	Details of the request
C4.T3.5	Access Rule Cited	This can be a link to the rule under which the request was made if that rule is kept in the system. If not, it can be a text field that captures the title, date, and version of the rule.
C4.T3.6	Request Date	Date request was received
Mandatory Support		
C4.T3.7.	User-defined Fields	

C4.1.4.2. Individual Access Request Time Limits. The RMA shall provide the capability for an authorized individual to set time limits that will apply to acknowledging requests for access and for providing access (see DoD 5400.11-R (C3.1.11), reference (av)).

C4.1.4.3. Tracking Individual Access Requests. RMAs shall provide authorized individuals the capability to track IARs.

C4.1.4.3.1. Assigning Suspense Dates. The RMA shall automatically assign acknowledgement and access grant suspense dates to the IAR by adding the relevant time limit to the “Request Date.” (see DoD 5400.11-R (C3.1.11), reference (av)).

C4.1.4.3.2. Workflow/Interim Suspense Dates. The RMA shall provide the capability for an authorized individual to assign the IAR to a workflow or to create and assign alert logic to user-defined interim suspense dates and extensions to suspense dates (see DoD 5400.11-R (C3.1.11), reference (av)).

C4.1.5. Managing Individual Access Requests. The RMA shall provide the capability for the authorized individual to capture and link authorization and denial decision documents or data to the IAR.

C4.1.5.1. Managing Individual Access Authorizations. The RMA shall provide the capability for an authorized individual to create record of actual individual accesses, including in-person access, authorized agent by mail access, by fax access, e-mail, and by Internet Access. Access data shall include the following:

Table C4.T4. Access Record Components

Requirement	**Access Record Component**	**Reference/ Comment**
Mandatory Data Collection		
C4.T4.1.	Access Type	One of a selection list that includes “In Person,

Table C4.T4. Access Record Components		
Requirement	**Access Record Component**	**Reference/ Comment**
		Authorized Agent, By Mail, By FAX, By E-mail, Via Internet."
C4.T4.2.	Access Date	In Person, the date the person visited. If Authorized Agent, the date the Agent visited, If By Mail, By FAX, or By Email, the date the package was sent, if Via Internet, the date the person logged in.
C4.T4.3.	Records Accessed	A listing of the records accessed by or provided to the individual.
C4.T4.4.	Record Description	A discussion of the record state, Original, redacted, summary, data collection, etc.
Mandatory Support		
C4.T4.5.	User-defined Fields	

C4.1.5.2. Record Collection. RMAs shall provide the capability for an authorized individual to search for and retrieve records meeting access request criteria.

C4.1.5.3. Providing Individual Access. The RMA shall provide interfaces with common office applications or document management systems to support the drafting of non-original documents such as redacted, summarized, reports, data listings. The RMA shall collect pertinent metadata from the office application or document management system file properties to pre-populate relevant metadata elements for filing these as new records.

C4.1.5.4. Managing Records Accessed. The RMA shall link the records accessed with the access record. In the case where non-original records such as redacted, summarized, reports, data listings, are created to provide access, RMAs shall prompt users to file them as new records. The RMA shall automatically link the new records to original records that were referenced, but not released for access.

C4.1.5.5. Preparing Individual Access Denials Notices. The RMA shall provide interfaces with common office applications or document management systems to support the drafting of denial notification documents. The RMA shall collect pertinent metadata from the office application or document management system file properties to pre-populate relevant metadata elements.

C4.1.5.5.1. Managing Individual Access Denials Metadata. The RMA shall provide the capability for an authorized individual to create a record of access denials (see DoD 5400.11-R (C3.2.3), reference (av)). Denial data shall include the following:

Table C4.T5. Denial Components		
Requirement	**Denial Component**	**Reference/ Comment**
Mandatory Data Collection		

Table C4.T5. Denial Components		
Requirement	**Denial Component**	**Reference/ Comment**
C4.T5.1.	Link to Access Request	
C4.T5.2.	Denial Authority	Name, title, position, signature or electronic signature of designated denial authority
C4.T5.3.	Denial Date	
C4.T5.4.	Denial Reason	Text or link to sections of laws, policies, or rules allowing denial.
C4.T5.5.	Appeal Suspense	60 calendar days from Denial Date. Suspense duration depends on published policy. 60 days is current DoD policy.
C4.T5.6.	Appeals Official	Name, title, position, signature or electronic signature of designated appeals authority
Mandatory Support		
C4.T5.7.	User-defined Fields	

C4.1.5.6. Managing Appeals. The RMA shall link the appeal record with the denial record(s).

C4.1.5.6.1. Managing Appeal Metadata. The RMA shall provide the capability for an authorized individual to create records of appeals (see DoD 5400.11-R (C3.2.4), reference (av)). Appeal data shall include the following:

Table C4.T6. Appeal Components		
Requirement	**Appeal Component**	**Reference/ Comment**
Mandatory Data Collection		
C4.T6.1.	Appeal ID	Unique identifier for this appeal.
C4.T6.2.	Denial ID Link	Link to denial being appealed
C4.T6.3.	Original Request ID Link	Link to original request
C4.T6.4.	Nature of Appeal	One of Review, Dispute, or Disclosure Accounting
C4.T6.5.	Details	Details of the appeal
C4.T6.6.	Appeal Date	Date Appeal was received
Mandatory Support		
C4.T6.7.	User-defined Fields	

C4.1.5.7. Appeal Time Limits. The RMA shall provide the capability for an authorized individual to set time limits that will apply to processing appeals (see DoD 5400.11-R (C3.2.4.5), reference (av)).

C4.1.5.8. Tracking Appeals.

C4.1.5.8.1. Assigning Suspense Dates. The RMA shall automatically assign acknowledgement and appeal response suspense dates to the appeal by adding the relevant time limit to the “Appeal Date.” (see DoD 5400.11-R (C3.2.4.5), reference (av)).

C4.1.5.8.2. Workflow/ Interim Suspense Dates. The RMA shall provide the capability for an authorized individual to assign the appeal to a workflow or to create and assign alert logic to user-defined interim suspense dates and extensions to suspense dates (see DoD 5400.11-R (C3.2.4.5, C3.2.5.3), reference (av)).

C4.1.5.9. Managing Amendment Requests. The RMA shall link the amendment request record with the record(s) to be amended(s).

C4.1.5.9.1. Managing Amendment Requests Metadata. The RMA shall provide the capability for an authorized individual to create a record of an amendment request (see DoD 5400.11-R (C3.3.2), reference (av)). Amendment request data shall include the following:

Table C4.T7. Amendment Components

Requirement	**Amendment Component**	**Reference/ Comment**
Mandatory Data Collection		
C4.T7.1.	Request ID	Unique identifier for this appeal.
C4.T7.2.	Record Link	Link to record(s) to be amended
C4.T7.3.	Amendment Justification	
C4.T7.4.	Amendment Type	One of Deletion Correction, Addition.
C4.T7.5.	Amendment Request Date	Date amendment request was received
C4.T7.6.	Reference Links	Links to records supplied by requestor as documentary evidence.
C4.T7.7	Amendment Resolution	How the amendment request was resolved
C4.T7.8	Amendment Resolution Date	Date request was resolved.
Mandatory Support		
C4.T7.9.	User-defined Fields	

C4.1.5.10. Amendment Request Time Limits. The RMA shall provide the capability for an authorized individual to set time limits that will apply to processing amendment requests (see DoD 5400.11-R (C3.3.7), reference (av)).

C4.1.5.11. Tracking Amendments.

C4.1.5.11.1. Assigning Suspense Dates. The RMA shall automatically assign acknowledgement and appeal response suspense dates to the appeal by adding the relevant time limit to the “Amendment Request Date” (see DoD 5400.11-R (C3.3.7), reference (av)).

C4.1.5.11.2. Workflow/ Interim Suspense Dates. The RMA shall provide the capability for an authorized individual to assign the amendment request to a workflow or to create and assign alert logic to user-defined interim suspense dates and extensions to suspense dates (see DoD 5400.11-R (C3.3.7), reference (av)).

C4.1.5.11.3. Previous Recipient Notification. RMAs shall provide links to relevant disclosure accounting records so that an authorized individual can identify previous recipients of the record and notify them of the amendment (see DoD 5400.11-R (C3.3.9), reference (av)).

C4.1.5.12. Managing Disputes/Statements of Disagreement. The RMA shall link the dispute or statement of disagreement record with the disputed record(s) and with the Amendment Request Record(s).

C4.1.5.13. Disputes/Statements of Disagreement Metadata. RMAs shall provide an authorized individual the capability to collect and manage metadata about Disputes and Disagreements as follows:

Table C4.T8. Dispute Components

Requirement	**Dispute Component**	**Reference/ Comment**
Mandatory Data Collection		
C4.T8.1.	Dispute ID	Unique identifier for this appeal.
C4.T8.2.	Disclosure ID	Link to disclosure record
C4.T8.3.	Dispute Author	Person initializing the dispute
C4.T8.4.	Dispute Date Received	Date organization received the dispute
C4.T8.5.	Dispute Date Closed	Date of final action on dispute
C4.T8.6.	Nature of Dispute	Summary of dispute allegations
C4.T8.7.	Discussion	Discussion of the dispute allegations
C4.T8.8.	Resolution	Discussion of the final resolution of the dispute.
Conditional Data Collection		
C4.T8.9.	Statement of Disagreement	Mandatory if dispute author provides a statement
C4.T8.10.	Civil Action	Mandatory if civil action arises from dispute
C4.T8.11.	Preparer	Identification of individual preparing disclosure or individual access response that led to dispute. Mandatory if dispute is related to a disclosure(s)
C4.T8.12.	Released By	Identification of person approving disclosure, or individual access response. Mandatory if dispute is related to a disclosure(s)
C4.T8.13.	Request ID	Link to original access request. Mandatory if dispute is related to a disclosure(s) or individual access response(s)
Mandatory Support		
C4.T8.14.	User-defined Fields	

C4.1.5.13.1. Disclosing Disputes. The RMA shall retrieve disputes or statements of disagreement with affected records when those records meet disclosure search criteria.

C4.1.6. Disclosures. RMAs shall provide authorized individuals the capability to record disclosure requests and track, manage, and account for disclosures (see DoD 5400.7-R and DoD 5400.11-R (C4), references (af) and (av)).

C4.1.6.1. Managing Disclosure Request Metadata. The RMA shall provide the capability for an authorized individual to create a record of a disclosure request. Disclosure request data shall include the following:

Table C4.T9. Disclosure Request Components

Requirement	**Disclosure Request Component**	**Reference/ Comment**
Mandatory Data Collection		
C4.T9.1.	Disclosure Request ID	Unique identifier for this request.
C4.T9.2.	Disclosure Requestor	Contact Information for the authorized agent requesting the disclosure
C4.T9.3.	Disclosure Purpose	Purpose to which the disclosed information will be put.
C4.T9.4.	Details	Details about the requested disclosure
C4.T9.5.	Disclosure Request Date	Date Disclosure Request was received
Conditional Data Collection		
C4.T9.9.	Individual Consent	Mandatory if consent is required, for requests that include individually identifying information.
Mandatory Support		
C4.T9.14.	User-defined Fields	

C4.1.6.2. Managing Disclosure Metadata. The RMA shall provide the capability for an authorized individual to create a record of a disclosure. Disclosure metadata shall include the following:

Table C4.T10. Disclosure Components

Requirement	**Disclosure Component**	**Reference/ Comment**
Mandatory Data Collection		
C4.T10.1.	Disclosure ID	Unique identifier for this Disclosure.
C4.T10.2.	Disclosure Request ID	Link to the Disclosure Request or NARA transfer identifier
C4.T10.3.	Disclosure Date	Date the disclosure was released to requestor.
C4.T10.4.	Disclosure Description	Description of the information released. This may also be links to actual records disclosed.
C4.T10.5.	Disclosure Notes	Discussion of deletions or changes to records disclosed. Also may be other information pertinent to the disclosure.
C4.T10.6.	Disclosure Purpose	Reason for Disclosure
C4.T10.7.	Disclosure Recipient	Name of recipient of disclosed records
C4.T10.8.	Disclosure Recipient Unit	Organization receiving disclosed records
C4.T10.9.	Preparer	The identification of the person responsible for preparing the disclosure
C4.T10.10.	Released By	The identification of the person responsible for releasing the information.
C4.T10.11.	Records Disclosed	A link to the records disclosed by this disclosure. If original records were redacted and new records created, this shall point to the actual records released.

Table C4.T10. Disclosure Components

Requirement	Disclosure Component	Reference/ Comment
C4.T10.12.	Dispute Information	Indicate if disclosed information has been corrected or disputed.
C4.T10.13.	System of Records	Link to System of records disclosure was made from
Conditional Data Collection		
C4.T10.14.	FOIA Request	Optional Link to FOIA Request. May generalize requests for both FOIA and Privacy Act if request requirements are sufficiently similar. One of the FOIA, Other, or Privacy Act request fields is mandatory, unless this is a NARA transfer.
C4.T10.15.	Other Request	Could be court order, subpoena, etc.
C4.T10.16.	Privacy Act Request	Optional Link to Privacy Act Request. May generalize requests for both FOIA and Privacy Act if request requirements are sufficiently similar
Mandatory Support		
C4.T10.17.	User-defined Fields	

C4.1.6.3. Tracking Disclosures. RMAs shall provide the capability for authorized individuals to manage and account for disclosures.

C4.1.6.3.1. Assigning Suspense Dates. The RMA shall provide the capability for an authorized individual to assign suspense dates to a disclosure request.”

C4.1.6.3.2. Workflow/ Interim Suspense Dates. The RMA shall provide the capability for an authorized individual to assign the disclosure request to a workflow or to create and assign alert logic to user defined interim suspense dates and extensions to suspense dates.

C4.1.6.3.3. Record Collection. RMAs shall provide the capability for an authorized individual to search for and retrieve records meeting disclosure request criteria. RMAs shall provide the capability for an authorized individual to create a copy of a retrieved record for redacting and/or summarizing.

C4.1.6.3.4. Preparing Disclosures. The RMA shall provide interfaces with common office applications or document management systems to support the drafting of disclosure documents. The RMA shall collect pertinent metadata from the office application or document management system file properties to pre-populate relevant metadata elements.

C4.1.6.3.5. Managing Redacted and Summarized Records. RMAs shall provide the capability for authorized individuals to link redacted versions of records and record summaries to the original records.

C4.1.6.4. Disclosure Accounting. RMAs shall provide authorized individuals with the capability to account for each disclosure of information from the SOR.

C4.1.6.4.1. Accounting Records. The RMA shall provide the capability for an authorized individual to create an accounting record. Accounting Record data shall include the following:

Table C4.T11. Accounting Record Components

Requirement	**Accounting Component**	**Reference/ Comment**
Mandatory Data Collection		
C4.T11.1.	Accounting ID	Unique identifier for this Account Record.
C4.T11.2.	Accounting Review Date	Date disclosure was reviewed
C4.T11.3.	Accounting Reviewed By	Name and contact information for person conducting the review
C4.T11.4.	Disclosure ID	Link to reviewed disclosure(s)
Conditional Data Collection		
C4.T11.5.	Accounting Release Date	Date accounting was released to individuals concerned.
C4.T11.6.	Individual Access Request	Link to access request if applicable
Mandatory Support		
C4.T11.7.	User-defined Fields	

C4.1.6.4.2. Linking Accounting Records to Disclosures. The RMA shall automatically link an accounting record to the disclosure being reviewed.

C4.1.6.5. Disclosure Exemptions. The RMA shall provide an authorized individual the capability to create and manage exemption records (see DoD 5400.7-R and DoD 5400.11-R (C5), references (af) and (av)).

C4.1.6.5.1. Exemption Records. The RMA shall provide the capability for an authorized individual to create an exemption record. Accounting Record data shall include the following:

Table C4.T12. Exemption Components

Requirement	**Exemption Component**	**Reference/ Comment**
Mandatory Data Collection		
C4.T12.1.	Exemption ID	Unique identifier for this Exemption
C4.T12.2.	Privacy Act Section Ref	Reference in the Privacy Act that allows the exemption
Conditional Data Collection		
C4.T12.3.	Privacy Act Text	Optional exemption text
C4.T12.4.	General Exemption	Optional exemption text
C4.T12.5.	Specific Exemption	Optional exemption text
Mandatory Support		
C4.T12.6.	User-defined Fields	

C4.1.6.5.2. Linking Exemptions to Records. The RMA shall provide an authorized individual the capability to link an exemption record to a record or a group of records.

C4.1.7. Matching Programs. The RMA shall provide an authorized individual the capability to create and manage matching program records (see DoD 5400.11-R (C11), reference (av)).

C4.1.7.1. Matching Program Records. The RMA shall provide the capability for an authorized individual to create a matching program record. Matching Program Record data shall include the following:

Table C4.T13. Matching Program Components

Requirement	**Matching Program Component**	**Reference/ Comment**
Mandatory Data Collection		
C4.T13.1.	Matching Program ID	Unique identifier for this Matching Program Record.
C4.T13.2.	Sibling System Identification	System Name or identifier of systems with which information will be cross-matched
C4.T13.3.	Sibling System POC	Matching Program Point of Contact for the other system
C4.T13.4.	Data Integrity Board	Composition of the board who oversees this matching program
C4.T13.5.	Purpose	Purpose of the matching program
C4.T13.6.	Notices	A link to any federal register notices of this matching program. In the case where the program is not-public, a link to reports about this program
Conditional Data Collection		
C4.T13.7.	Adverse Actions	Adverse actions that can be levied on members of the public as a result of the information matches found by this matching program. Mandatory if applicable.
Mandatory Support		
C4.T13.8.	User-defined Fields	

C4.1.7.2. Linking Matching Programs to SORs. The RMA shall provide an authorized individual the capability to link matching program record to the referenced system of records.

C4.1.7.3. Preparing Matching Program Notices. The RMA shall provide interfaces with common office applications or document management systems to support the drafting of matching program notices. The RMA shall collect pertinent metadata from the office application or document management system file properties to pre-populate relevant metadata elements.

C4.1.8. Electronic Privacy Act Elements (Optional). RMAs shall provide graphical user interface capabilities to allow authorized individuals to create and publish web portals to support electronic Privacy Act requests.

C4.2. MANAGEMENT OF FREEDOM OF INFORMATION ACT RECORDS

C4.2.1. The following requirements are mandatory for only those RMAs that support the Freedom of Information Act (FOIA). Organizational compliance to FOIA may be implemented outside the scope of an RMA. These requirements are in addition to those requirements outlined in Chapters 2 and 3. In this chapter, the word "shall" identifies mandatory system standards for managing FOIA records. The word "should" identifies design objectives that are desirable but not mandatory. Additionally, requirements for safeguarding and providing security for FOIA records are not in the scope of this document, since they are provided in other directives and regulations.

C4.2.2. Organization Access Rules. RMAs shall provide functionality that supports authorized personnel in preparing and posting access rules for the public to gain access to FOIA information.

C4.2.2.1. Access Rule Metadata. The RMA shall provide the capability for an authorized individual to create an access rules record. Access Rules data shall include the following:

Table C4.T14. Access Rules Components

Requirement	**Access Rules Component**	**Reference/ Comment**
Mandatory Data Collection		
C4.T14.1.	FOIA Rule Identifier	Unique identifier for this Access Rule document.
C4.T14.2.	Access Rules	Pointer to the rules document. The requirements for capturing information about and publishing access rules may be similar enough between Privacy Act and FOIA to share one set of metadata elements for other metadata.

C4.2.2.2. Preparing Access Rules. The RMA shall provide interfaces with common office applications or document management systems to support the drafting of access rules documents. The RMA shall collect pertinent metadata from the office application or document management system file properties to pre-populate relevant metadata elements.

C4.2.3. FOIA Access Requests. RMAs shall provide functionality that supports authorized personnel in recording, tracking and managing a FOIA request.

C4.2.3.1. FOIA Request Metadata[3]. At a minimum the RMA shall support the collection of the following FOIA metadata and store and manage the request as a record.

Table C4.T15. FOIA Request Components		
Requirement	**FOIA Request Component**	**Reference/ Comment**
Mandatory Data Collection		
C4.T15.1.	Request ID	Unique identifier for this request
C4.T15.2.	Request Author	Identification and contact information for person requesting information
C4.T15.3.	Nature of Request	Summary of request focus
C4.T15.4.	Details	Details of the request
C4.T15.5.	Access Rule Cited	This can be a link to the rule under which the request was made if that rule is kept in the system. If not, it can be a text field that captures the title, date, and version of the rule.
C4.T15.6.	Request Date	Date request was received
Mandatory Support		
C4.T15.7.	User-defined Fields	

C4.2.3.2. FOIA Request Time Limits. The RMA shall provide the capability for an authorized individual to set time limits that will apply to acknowledging requests for access and for providing access.

C4.2.3.3. Tracking FOIA Requests. RMAs shall provide authorized individuals the capability to track FOIA Requests.

C4.2.3.3.1. Assigning Suspense Dates. The RMA shall automatically assign acknowledgement and access grant suspense dates to the FOIA request by adding the relevant time limit to the “Request Date.”

C4.2.3.3.2. Workflow/Interim Suspense Dates. The RMA shall provide the capability for an authorized individual to assign the FOIA request to a workflow or to create and assign alert logic to user defined interim suspense dates and extensions to suspense dates.”

C4.2.4. Disclosures. RMAs shall provide authorized individuals the capability to record disclosure requests and track, manage, and account for disclosures (see DoD 5400.7-R and DoD 5400.11-R (C4), references (af) and (av)).

[3] Note that FOIA requests and Privacy Act Individual Access Requests are very similar. One object could be used to support both.

C4.2.4.1. Managing Disclosure Request Metadata. The RMA shall provide the capability for an authorized individual to create a record of a FOIA disclosure request. Disclosure metadata shall include the following:

Table C4.T16. FOIA Disclosure Request Components

Requirement	FOIA Disclosure Request Component	Reference/ Comment
Mandatory Data Collection		
C4.T16.1.	Disclosure Request ID	Unique identifier for this request.
C4.T16.2.	Disclosure Requestor	Contact information for the authorized agent requesting the disclosure.
C4.T16.3.	Details	Details about the requested disclosure, (i.e. which records).
C4.T16.4.	Disclosure Request Date	Date Disclosure Request was received.
Conditional Data Collection		
C4.T16.5.	Disclosure Purpose	Purpose to which the disclosed information will be put.
C4.T16.6.	Individual Consent	Some disclosures require individual consent. This field could link to that consent document.
Mandatory Support		
C4.T16.7.	User-defined Fields	User-defined fields may be used to capture extra information, including whether or not the FOIA disclosure request was denied.

C4.2.4.2. Managing Disclosure Metadata. The RMA shall provide the capability for an authorized individual to create a record of a FOIA disclosure. Disclosure metadata shall include the following:

Table C4.T17. FOIA Disclosure Components

Requirement	FOIA Disclosure Component	Reference/ Comment
Mandatory Data Collection		
C4.T17.1.	Disclosure ID	Unique identifier for this Disclosure.
C4.T17.2.	Disclosure Request ID	Link to the Disclosure Request or NARA transfer identifier
C4.T17.3.	Disclosure Date	Date the disclosure was released to requestor.
C4.T17.4.	Disclosure Description	Description of the information released. This may also be links to actual records disclosed.
C4.T17.5.	Disclosure Notes	Discussion of deletions or changes to records disclosed. Also may be other information pertinent to the disclosure.
C4.T17.6.	Disclosure Purpose	Reason for Disclosure
C4.T17.7.	Disclosure Recipient	Name of recipient of disclosed records
C4.T17.8.	Disclosure Recipient Unit	Organization receiving disclosed records
C4.T17.9.	Preparer	The identification of the person responsible for preparing the disclosure
C4.T17.10.	Released By	The identification of the person responsible for releasing the information.
C4.T17.11.	Records Disclosed	A link to the records disclosed by this disclosure.

Table C4.T17. FOIA Disclosure Components

Requirement	FOIA Disclosure Component	Reference/ Comment
		If original records were redacted and new records created, this shall point to the actual records released.
C4.T17.12.	Dispute Information	Indicate if disclosed information has been corrected or disputed.
C4.T17.13.	System of Records	Link to System of records disclosure was made from
Conditional Data Collection		
C4.T17.14.	FOIA Request	Optional Link to FOIA Request. May generalize requests for both FOIA and Privacy Act if request requirements are sufficiently similar. One of the FOIA, Other, or Privacy Act request fields is mandatory, unless this is a NARA transfer.
C4.T17.15.	Other Request	Could be court order, subpoena, etc. One of the FOIA, Other, or Privacy Act request fields is mandatory, unless this is a NARA transfer.
C4.T17.16.	Privacy Act Request	Optional Link to Privacy Act Request. May generalize requests for both FOIA and Privacy Act if request requirements are sufficiently similar. One of the FOIA, Other, or Privacy Act request fields is mandatory, unless this is a NARA transfer.
Mandatory Support		
C4.T17.17.	User-defined Fields	

C4.2.4.3. Tracking Disclosures. RMAs shall provide the capability for authorized individuals to manage and account for disclosures.

C4.2.4.3.1. Assigning Suspense Dates. The RMA shall provide the capability for an authorized individual to assign suspense dates to a FOIA request.”

C4.2.4.3.2. Workflow/ Interim Suspense Dates. The RMA shall provide the capability for an authorized individual to assign the FOIA request to a workflow or to create and assign alert logic to user defined interim suspense dates and extensions to suspense dates.

C4.2.4.3.3. Record Collection. RMAs shall provide the capability for an authorized individual to search for and retrieve records meeting FOIA request criteria. RMAs shall provide the capability for an authorized individual to create a copy of a retrieved record for redacting and/or summarizing.

C4.2.4.3.4. Preparing Disclosures. The RMA shall provide interfaces with common office applications or document management systems to support the drafting of disclosure documents. The RMA shall collect pertinent metadata from the office application or document management system file properties to pre-populate relevant metadata elements.

C4.2.4.3.5. Managing Redacted and Summarized Records. RMAs shall provide the capability for authorized individuals to link redacted versions of records and record summaries to the original records.

C4.2.4.4. Disclosure Exemptions. The RMA shall provide an authorized individual the capability to create and manage exemption records (see DoD 5400.7-R and DoD 5400.11-R (C5), references (af) and (av)).

C4.2.4.4.1. Exemption Records. The RMA shall provide the capability for an authorized individual to create an exemption record. Exemption Record data shall include the following:

Table C4.T18. FOIA Exemption Components

Requirement	**Exemption Component**	**Reference/ Comment**
Mandatory Data Collection		
C4.T18.1.	Exemption ID	Unique identifier for this Exemption
C4.T18.2.	FOIA Section Ref	Reference in the legal documentation that allows the exemption
Conditional Data Collection		
C4.T18.3.	Privacy Act Text	Optional exemption text
C4.T18.4.	General Exemption	Optional exemption text
C4.T18.5.	Specific Exemption	Optional exemption text
Mandatory Support		
C4.T18.6.	User-defined Fields	

C4.2.4.4.2. Linking Exemptions to Records. The RMA shall provide an authorized individual the capability to link an exemption record to a record or a group of records.

C4.2.4.5. Managing Appeals. The RMA shall link the appeal record with the denial record(s).

C4.2.4.5.1. Managing Appeal Metadata. The RMA shall provide the capability for an authorized individual to create a record of appeals. Appeal data shall include the following:

Table C4.T19. FOIA Appeal Components

Requirement	**FOIA Appeal Component**	**Reference/ Comment**
Mandatory Data Collection		
C4.T19.1.	Appeal ID	Unique identifier for this appeal.
C4.T19.2.	FOIA Disclosure	Link to disclosure record
C4.T19.3.	Appeal Author	
C4.T19.4.	Appeal Date Received	Date appeal was received

Table C4.T19. FOIA Appeal Components		
Requirement	**FOIA Appeal Component**	**Reference/ Comment**
C4.T19.5.	Appeal Date Closed	Date appeal was closed
C4.T19.6.	Appeal Justification	Justification for Appeal
C4.T19.7	Appeal Resolution	Date the appeal was resolved
C4.T19.8	Appeal Preparer	Name of person preparing response to appeal
C4.T19.9	Released By	Authority for releasing response to appeal
C4.T19.10	FOIA Request	Link to original request record
Conditional Data Collection		
C4.T19.11	Discussion	Mandatory if critical to documenting appeal
Mandatory Support		
C4.T19.12.	User-defined Fields	

C4.2.4.6. Appeal Time Limits. The RMA shall provide the capability for an authorized individual to set time limits that will apply to processing appeals.

C4.2.4.7. Tracking Appeals.

C4.2.4.7.1. Assigning Suspense Dates. The RMA shall automatically assign acknowledgement and appeal response suspense dates to the appeal by adding the relevant time limit to the "Appeal Date."

C4.2.4.7.2. Workflow/ Interim Suspense Dates. The RMA shall provide the capability for an authorized individual to assign the appeal to a workflow or to create and assign alert logic to user-defined interim suspense dates and extensions to suspense dates.

C4.2.5. FOIA Reports. RMAs shall provide authorized individuals the capability to create, file, and manage FOIA Reports.

C4.2.5.1. FOIA Reports Metadata. At a minimum the RMA shall capture the following FOIA report metadata:

Table C4.T20. Disclosure Components		
Requirement	**Disclosure Component**	**Reference/ Comment**
Mandatory Data Collection		
C4.T20.1.	Denials	Number of determinations made to deny requests for records and the reasons for those denials.
C4.T20.2.	Appeals	Results of appeals
C4.T20.3.	Requests Pending	Number of requests pending from previous year
C4.T20.4.	Requests Received	Number of requests received in current year
C4.T20.5.	Request Processed	Number of requests processed in current year.
C4.T20.6.	Processing Time	Median number of days to process different types of requests
C4.T20.7.	Total Fees	Amount of fees collected for fulfilled requests.
C4.T20.8.	Staff Allocated	Number of fulltime staff dedicated to FOIA in

Table C4.T20. Disclosure Components		
Requirement	**Disclosure Component**	**Reference/ Comment**
		current year
C4.T20.9.	Amount expended	Total amount expended to meet FOIA requirements.
Mandatory Support		
C4.T20.10.	User-defined Fields	

C4.2.5.2. FOIA Reporting Links. RMAs shall be able to link the following to the FOIA report:

C4.2.5.2.1. Requests.

C4.2.5.2.2. Appeals.

C4.2.5.2.3. Denials.

C4.2.5.2.4. Other records or metadata objects used in creating the report.

C4.2.6. Electronic FOIA Elements (Optional). RMAs shall provide graphical user interface capabilities to allow authorized individuals to create and publish web portals to support electronic FOIA requests.

C4.3. ACCESS CONTROL

C4.3.1. Table C34.T21. summarizes requirements that refer to "authorized individuals" and offers additional information regarding user-type responsibilities. In general, Application Administrators are responsible for setting up the RMA infrastructure. Records Managers are responsible for records management administration. Privileged Users are those who are given special permissions to perform functions beyond those of typical users.

Table C4.T21. Authorized Individual Requirements			
Requirement	**Application Administrator**	**Records Manager**	**Privileged User**
C4.1.3. Privacy Case Files. …create and manage Privacy Case Files.	NA	Create and Manage	Create and Manage
C4.1.4.2. Individual Access Request Time Limits … set time limits that will apply to acknowledging requests for access and for providing access.	At Set Up	Set Time Limits	NA
C4.1.4.3. Tracking Individual Access Requests … track IARs.	NA	Track	Track

Table C4.T21. Authorized Individual Requirements			
Requirement	**Application Administrator**	**Records Manager**	**Privileged User**
C4.1.4.3.2. Workflow/Interim Suspense Dates … assign the IAR to a workflow or to create and assign alert logic to user-defined interim suspense dates and extensions to suspense dates.	Create Logic	Create Logic/Assign Workflow	Assign Workflow
C4.1.5. Managing Individual Access Requests … capture and link authorization and denial decision documents or data to the IER.	NA	Link/Unlink	Link
C4.1.5.1. Managing Individual Access Authorizations … create record of actual individual accesses…	NA	Create, Edit, Destroy record	Create Record
C4.1.5.2. Record Collection …search for and retrieve records	NA	Search/Retrieve	Search/Retrieve
C4.1.5.5.1. Managing Individual Access Denials Metadata …create record of access denials.	NA	Create, Edit, Destroy record	Create Record
C4.1.5.6.1. Managing Appeal Metadata … create records of appeals.	NA	Create, Edit, Destroy record	Create Record
C4.1.5.7. Appeal Time Limits … set time limits that will apply to processing appeals.	At Set Up	Set Time Limits	NA
C4.1.5.8.2. Workflow/ Interim Suspense Dates … assign the appeal to a workflow or to create and assign alert logic to user-defined interim suspense dates and extensions to suspense dates.	Create Logic	Create Logic/Assign Workflow	Assign Workflow
C4.1.5.9.1. Managing Amendment Requests Metadata …create a record of an amendment request.	NA	Create, Edit, Destroy record	Create Record
C4.1.5.11.2. Workflow/ Interim Suspense Dates …assign the amendment request to a workflow or to create and assign alert logic to user-defined interim suspense dates and extensions to suspense dates.	Create Logic	Create Logic/Assign Workflow	Assign Workflow
C4.1.5.11.3. Previous Recipient Notification … identify previous recipients of the record and notify them of the amendment.	NA	Create/Edit/Run Disclosure Accounting	Run Disclosure Accounting
C4.1.5.13 Disputes/Statements of Disagreement Metadata …collect and manage metadata about Disputes and Disagreements	NA	Create, Edit, Destroy record	Create Record

Table C4.T21. Authorized Individual Requirements			
Requirement	**Application Administrator**	**Records Manager**	**Privileged User**
C4.1.6. Disclosures … record disclosure requests and track, manage, and account for disclosures.	NA	Create/Edit/Run Disclosure Accounting	Run Disclosure Accounting
C4.1.6.1. Managing Disclosure Request Metadata … create a record of a disclosure request. :	NA	Create, Edit, Destroy record	Create Record
C4.1.6.1.2. Managing Disclosure Metadata … create a record of a disclosure.	NA	Create, Edit, Destroy record	Create Record
C4.1.6.3. The RMA shall provide the capability for Tracking Disclosures … manage and account for disclosures.	NA	Create/Edit/Run Disclosure Accounting	Run Disclosure Accounting
C4.1.6.3.1 Assigning Suspense Dates … assign suspense dates to a disclosure request."	Create Logic	Create Logic/Assign Workflow	Assign Workflow
C4.1.6.3.2 Workflow/ Interim Suspense Dates … assign the disclosure request to a workflow or to create and assign alert logic to user defined interim suspense dates and extensions to suspense dates.	Create Logic	Create Logic/Assign Workflow	Assign Workflow
C4.1.6.3.3 Record Collection … search for and retrieve records meeting disclosure request criteria. … create a copy of a retrieved record for redacting and/or summarizing.	NA	Search/Retrieve	Search/Retrieve
C4.1.6.3.5 Managing Redacted and Summarized Records … link redacted versions of records and record summaries to the original records.	NA	Link/Unlink	Link
C4.1.6.4 Disclosure Accounting … account for each disclosure of information from the SOR.	NA	Create/Edit/Run Disclosure Accounting	Run Disclosure Accounting
C4.1.6.4.1 Accounting Records … create an accounting record. :	NA	Create, Edit, Destroy record	Create Record
C4.1.6.5 Disclosure Exemptions … create and manage exemption records.	NA	Create, Edit, Destroy record	Create Record
C4.1.6.5.1 Exemption Records … create an exemption record:	NA	Create, Edit, Destroy record	Create Record
C4.1.6.5.2 Linking Exemptions to Records … link an exemption record to a record or a group of records.	NA	Link/Unlink	Link
C4.1.7. Matching Programs … create and manage matching program records.	NA	Create, Edit, Destroy record	Create Record
C4.1.7.1. Matching Program Records … create a matching program record.	NA	Create, Edit, Destroy record	Create Record

Table C4.T21. Authorized Individual Requirements

Requirement	**Application Administrator**	**Records Manager**	**Privileged User**
C4.1.7.2. Linking Matching Programs to SORs … link matching program record to the referenced system of records.	NA	Link/Unlink	Link
C4.1.8. Electronic Privacy Act Elements (optional) … create and publish web portals to support electronic Privacy Act requests.	Create Page	Create Edit Pages	None
C4.2.2.1. Access Rule Metadata … create an access rules record.	NA	Create, Edit, Destroy record	Create Record
C4.2.3.2. FOIA Request Time Limits … set time limits that will apply to acknowledging requests for access and for providing access.	At Set Up	Set Time Limits	NA
C4.2.3.3. Tracking FOIA Requests … track FOIA Requests.	NA	Track	Track
C4.2.3.3.2. Workflow/Interim Suspense Dates … assign the FOIA request to a workflow or to create and assign alert logic to user defined interim suspense dates and extensions to suspense dates."	Create Logic	Create Logic/Assign Workflow	Assign Workflow
C4.2.4. Disclosures … record disclosure requests and track, manage, and account for disclosures	NA	Create, Edit, Destroy record	Create Record
C4.2.4.1.Managing Disclosure Request Metadata …create a record of a FOIA disclosure request.	NA	Create, Edit, Destroy record	Create Record
C4.2.4.2.Managing Disclosure Metadata … create a record of a FOIA disclosure.	NA	Create, Edit, Destroy record	Create Record
C4.2.4.3. Tracking Disclosures … manage and account for disclosures.	NA	Create/Edit/Run Disclosure Accounting	Run Disclosure Accounting
C4.2.4.3.1. Assigning Suspense Dates … assign suspense dates to a FOIA request."	Create Logic	Create Logic/Assign Workflow	Assign Workflow
C4.2.4.3.2. Workflow/ Interim Suspense Dates … assign the FOIA request to a workflow or to create and assign alert logic to user defined interim suspense dates and extensions to suspense dates.	Create Logic	Create Logic/Assign Workflow	Assign Workflow

Table C4.T21. Authorized Individual Requirements			
Requirement	**Application Administrator**	**Records Manager**	**Privileged User**
C4.2.4.3.3. Record Collection … search for and retrieve records meeting FOIA request criteria. … create a copy of a retrieved record for redacting and/or summarizing.	NA	Search/Retrieve	Search/Retrieve
C4.2.4.3.5. Managing Redacted and Summarized Records … link redacted versions of records and record summaries to the original records.	NA	Link/Unlink	Link
C4.2.4.4. Disclosure Exemptions … create and manage exemption records.	NA	Create, Edit, Destroy record	Create Record
C4.2.4.4.1. Exemption Records … create an exemption record. :	NA	Create, Edit, Destroy record	Create Record
C4.2.4.4.2. Linking Exemptions to Records … link an exemption record to a record or a group of records.	NA	Link/Unlink	Link
C4.2.4.5.1. Managing Appeal Metadata … create record of appeals.	NA	Create, Edit, Destroy record	Create Record
C4.2.4.6. Appeal Time Limits … set time limits that will apply to processing appeals.	At Set Up	Set Time Limits	NA
C4.2.4.7.2. Workflow/ Interim Suspense Dates … assign the appeal to a workflow or to create and assign alert logic to user-defined interim suspense dates and extensions to suspense dates.	Create Logic	Create Logic/Assign Workflow	Assign Workflow
C4.2.5. FOIA Reports. … create, file, and manage FOIA Reports.	NA	Create, Edit, Destroy record	Create Record
C4.2.6. Electronic FOIA Elements (optional) … create and publish web portals to support electronic FOIA requests.	Create Page	Create Edit Pages	None

(This page intentionally left blank.)

C5. CHAPTER 5

TRANSFERS

C5.1. TRANSFER RMA-RMA INTEROPERABILITY

C5.1.1. A record to be transferred may still be in its active lifecycle. As such it needs to be linked to sufficient information to allow continued tracking either by the receiving organization or by the originating organization using a new RMA. This Standard defines two levels of transfer. Mandatory transfer involves records and record folders. All RMAs are required to provide this capability. Optionally, RMAs should transfer file plans and links to the file plan context of a record or record folder. File Plan transfers shall follow the guidance in Paragraph C5.3.

C5.1.2. Context Management. RMAs shall support maintaining the transferred records' context.

C5.1.2.1. Writing Out Context. RMAs shall write out record metadata and content, including contextual links to other records in the transfer set. RMAs shall include the records' or record folders' lifecycle status.

C5.1.2.2. Ingesting Context. RMAs shall ingest record metadata and content and restore contextual links to other records in the transfer set as well as the record's status in its lifecycle.

C5.1.3. User-defined Optional Metadata Interoperability. User-defined elements are necessary to support a variety of agency functions. RMAs shall support definition, writing out, ingesting and linking of user-defined metadata elements to required elements and to affected records and record groupings.

C5.1.3.1. Support of User-Defined Elements. RMAs shall provide capabilities for defining, capturing data, storing, writing out, ingesting, and linking user-defined metadata elements to other elements as specified in this standard.

C5.1.4. Transfer Schema Structure. RMAs shall support reading from and writing to a standard transfer structure.

C5.1.4.1. Transfer Schema Default. RMAs shall support the current version of the DoD 5015.2-STD Transfer Schema. The initial version of the schema is included as Appendix A for mandatory elements, and Appendix B for optional elements. Vendors shall contact JITC for the most current version.

C5.1.4.2. Transfer Schema User-Defined. RMAs shall provide a graphical user interface capability for an authorized individual to add to or remove from the schema user-defined, defined optional, and any vendor provided metadata fields.

C5.1.5. Transfer Schema Metadata Mapping. RMAs shall support mapping metadata defined in this standard to the archival and transfer schemas.

C5.1.5.1. Transfer Schema Metadata Default Mapping. By default RMAs shall map metadata defined by this standard to the same named element in the archival and transfer schemas.

C5.1.5.2. Transfer Schema Metadata User-Defined Mapping. RMAs shall provide a graphical user interface capability to allow an authorized individual to map metadata to schema elements to support export and ingest. RMAs shall not allow users to override default mapping of mandatory metadata elements for export.

C5.1.6. User-Defined Elements Export Schemas and Rendering Aids. RMAs shall provide schema extensions for all system and user-defined metadata elements, attributes, and acceptable values for all metadata that may be exported. Such schema extensions may be provided in the form of extensions to the DDMS (reference (c)). RMAs shall provide the capability for an authorized individual to implement an export schema based on this standard and the vendor provided DTD. RMA-provided export DTDs and schemas shall not cause namespace conflicts with the metadata elements and attributes defined in this standard. RMAs shall include the Export DTD and export schemas as part of the transfer as a default. RMAs shall allow an authorized individual to remove the default if not needed by recipient. If required for proper metadata content rendering and presentation of metadata context, or as appropriate, RMAs shall provide Cascading Style Sheets or another open-standard rendering aid such as XSLT transformations as a component of the transfer.

C5.1.7. Record Elements. RMAs shall manage writing out records for transfer with the metadata shown in the following paragraphs. RMAs shall parse and process all metadata elements during ingestion. Optionally RMAs shall provide authorized individuals with graphical user interface capabilities to support merging ingested records into existing file plans.

C5.1.7.1. Standard Record Elements. RMAs shall write out metadata with records in the standard transfer formats. RMAs shall parse, ingest and link received standard formatted record information into the receiving database and/or repository.

C5.1.8. Record Elements.

C5.1.8.1. Record Level Core Elements. RMAs shall associate core elements with all records no matter the type or source.

C5.1.8.1.1. Record Level Core Mandatory. RMAs shall write out and ingest the following metadata and content elements for each record being transferred.

Table C5.T1. Record Level Core (Defined Mandatory)

Data Element	**Data Source**	**Content, Reference and Notes**
Record		
Record Identifier	RMA generated based on NARA assigned organizational identifiers. Paragraph C2.T3.1	Unique record identifier
Folder Identifier	RMA generated Paragraph C2.T2.1.2.	Foreign Key from Folder Grouping Level May be replaced by grouping for NARA archival action.
Title	RMA captured Paragraph C2.T3.2	Name of record Required by DoD 5015.2
Creator	RMA captured Paragraph C2.T3.5	Creator in LCDRG and in Dublin Core Person/Organization creating record Author in DoD 5015.2
Media	RMA captured Paragraph C2.T3.8	Physical manifestation of record. DoD 5015.2
Format	RMA captured Paragraph C2.T3.9	Electronic File Application Type. Binding or grouping of physical records DoD 5015.2
Date Published	RMA captured Paragraph C2.T3.4	Date Created in LCDRG and Dublin Core Date Released/Published DoD 5015.2
Link to supporting records/files	RMA captured Paragraph C2.2.3.17	Links to other records/files that are necessary to properly render this content. DoD 5015.2. Not record-record links for context.
Original Content	RMA captured Paragraph C2.2.3.1	Embedded original computer file content
Open Content	RMA shall prompt user to create an XML file if one does not already exist.	Embedded XML content. This is the original record content file converted to XML.

C5.1.8.2. E-mail. RMAs shall write out and ingest additional information from e-mail messages. These elements are in addition to core record elements.

C5.1.8.2.1. Record Level E-mail Mandatory. RMAs shall write out and ingest the following mandatory metadata for each e-mail record being transferred.

Table C5.T2. Record Level E-mail (Defined Mandatory)

Data Element	**Data Source**	**Content, Reference and Notes**
Record Email	NA	

Table C5.T2. Record Level E-mail (Defined Mandatory)		
Data Element	**Data Source**	**Content, Reference and Notes**
Record Identifier	RMA Generated Paragraph C2.T3.1	Link to Core mandatory elements
Sender	RMA captured Paragraph C2.T3.5	SMTP “From” element
Primary Addresses	RMA captured Paragraph C2.T3.11	SMTP “To” element
Secondary Addresses	RMA captured Paragraph C2.T3.12	SMTP “CC” element
Hidden Addresses	RMA captured Paragraph C2.T3.12	SMTP “BCC” element
Subject	RMA captured Paragraph C2.T3.2	From Email Subject.
Sent Timestamp	RMA captured. Paragraph C2.T4	Time email left server.
Received Timestamp	If filed on receipt, RMA captured from email header. Paragraph C2.T3.10	If filed on receipt, time email is received on server.
Attachment reference	RMA Generated Paragraph C2.2.4.3	If attachment(s)

C5.1.8.2.2. Record Level Mandatory for Records to be Transferred to NARA.

C5.1.8.2.2.1. Scanned Records. RMAs shall write out and ingest the following mandatory metadata for each scanned record being transferred to NARA.

Table C5.T3. Record Level Scanned (Defined Mandatory)		
Data Element	**Data Source**	**Content, Reference and Notes**
Record Scanned	NA	
Record Identifier	RMA Generated Paragraph C2.T3.1	
Scanned Image Format and Version	RMA captured Paragraph C2.T5.1.	NARA allows one of the following only; check with NARA for changes: TIFF 4.0 TIFF 5.0 TIFF 6. GIF 87a GIF 89a ISO 12087-5 PNG 1.0
Image Resolution	RMA captured Paragraph C2.T5.2	Image resolution relative to image encoding standard

C5.1.8.2.2.2. PDF Records. RMAs shall write out and ingest the following mandatory metadata for each PDF record being transferred to NARA.

Table C5.T4. Record Level PDF (Defined Mandatory)

Data Element	**Data Source**	**Content, Reference and Notes**
Record PDF	NA	
Record Identifier	RMA Generated Paragraph C2.T3.1	
Producing Application	RMA captured Paragraph C2.T5.3.	Application used to render content to PDF
Producing Application Version	RMA captured Paragraph C2.T5.4	
PDF Version	RMA captured Paragraph C2.T5.5	NARA allows versions 1.0 through 1.4 only; check with NARA for changes.

C5.1.8.2.2.3. Digital Photographs. RMAs shall write out and ingest the following mandatory metadata for each digital photograph record being transferred to NARA.

Table C5.T5. Record Level Digital Photograph (Defined Mandatory)

Data Element	**Data Source**	**Content, Reference and Notes**
Record Digital Photograph	N/A	
Record Identifier	RMA Generated Paragraph C2.T3.1	
Caption	RMA captured Paragraph C2.T5.6.	Narrative text describing each individual image in order to understand and retrieve it. Standard caption information typically includes the "who, what, when, where, why" about the photograph

C5.1.8.2.2.4. Web Records. RMAs shall write out and ingest the following mandatory metadata for each web record being transferred to NARA.

Table C5.T6. Record Level Web Records (Defined Mandatory)

Data Element	**Data Source**	**Content, Reference and Notes**
Record Web Record	N/A	
Record Identifier	RMA Generated Paragraph C2.T3.1	
File Name	RMA captured Paragraph C2.T5.7.	The file name of each web site file shall not exceed 99 ASCII characters, and with the path the name shall not exceed 254 ASCII characters.
Web Platform	RMA captured Paragraph C2.T5.8.	Include the specific software applications and where available intended browser applications and versions.
Web Site Name	RMA captured Paragraph C2.T5.9.	Title of the website from the main entry page.
Web Site URL	RMA captured	Include the filename of the starting page of the transferred

Table C5.T6. Record Level Web Records (Defined Mandatory)		
Data Element	**Data Source**	**Content, Reference and Notes**
	Paragraph C2.T5.10.	content.
Capture Method	RMA captured Paragraph C2.T5.11.	Include name and description of harvester iv used. If PDF, include the software and version used to capture the PDF. If more than one clearly identify which content was captured by which method.
Capture Date	RMA captured Paragraph C2.T5.12.	Date record was captured.
Contact	RMA captured Paragraph C2.T5.13.	Point of Contact information for person responsible for capturing the web record.

C5.1.8.2.3. Record Level Defined Optional for Records to be transferred to NARA. RMAs shall write out and ingest the following defined optional metadata for each record being transferred to NARA.

C5.1.8.2.3.1. Scanned Records. RMAs shall write out and ingest the following defined optional metadata for each scanned record being transferred to NARA when it is used.

Table C5.T6. Record Level Scanned (Defined Optional)		
Data Element	**Data Source**	**Content, Reference and Notes**
Record Scanned Optional	N/A	
Record Identifier	RMA Generated Paragraph C2.T3.1	
Image Bit Depth	RMA captured Paragraph C2.T5.14	Bit Depth relative to image encoding standard.

C5.1.8.2.3.2. PDF Records. RMAs shall write out and ingest the following defined optional metadata for each PDF record being transferred to NARA when it is used.

Table C5.T7. Record Level PDF (Defined Optional)		
Data Element	**Data Source**	**Content, Reference and Notes**
Record PDF Optional	N/A	
Record Identifier	RMA Generated Paragraph C2.T3.1	
Creating Application	RMA captured Paragraph C2.T5.15.	Application used to create initial record content, includes version.
Document Security Settings	RMA captured Paragraph C2.T5.16.	Additional Security added during PDF rendering.

C5.1.8.2.3.3. Digital Photographs. RMAs shall write out and ingest the following defined optional metadata for each digital photograph record being transferred to NARA when it is used

Table C5.T8. Record Level Digital Photograph (Defined Optional)		
Data Element	**Data Source**	**Content, Reference and Notes**
Record Digital Photograph Optional	N/A	
Record Identifier	RMA Generated Paragraph C2.T3.1	
Photographer	RMA captured Paragraph C2.T5.17.	Identify the full name (and rank, if military) and organization (agency, if Federal) of the photographer credited with the photograph, if available.
Copyright	RMA captured Paragraph C2.T5.18.	Indicate for each image whether there is a restriction on the use of that image because of a copyright or other property rights. Agencies must provide, if applicable, the owner of the copyright and any conditions on the use of the photograph(s), such as starting and ending dates of the restriction.
Bit Depth	RMA captured Paragraph C2.T5.19.	Identify the bit depth of the transferred files.
Image Size	RMA captured Paragraph C2.T5.20.	Specify the image height and width of each image in pixels
Image Source	RMA captured Paragraph C2.T5.21.	Identify the original medium used to capture the images
Compression	RMA captured Paragraph C2.T5.22.	Identify the file compression method used (if applicable) and the compression level (e.g., medium, high) selected for the image(s).
ICCM/ICM profile	RMA captured Paragraph C2.T5.23.	Provide custom or generic color profiles, if available, for the digital camera or scanner used [e.g., sRGB (standard Red Green Blue)].
EXIF Information	RMA captured Paragraph C2.T5.24.	If available, preserve and transfer to NARA the Exchangeable Image File Format (EXIF) information embedded in the header of image files (as TIFF tags or JPEG markers) by certain digital cameras (e.g., make and model of the digital camera).

C5.1.8.2.3.4. Web Records. RMAs shall write out and ingest the following defined optional metadata for each web record being transferred to NARA when it is used.

Table C5.T9. Record Level Web Record (Defined Optional)		
Data Element	**Data Source**	**Content, Reference and Notes**
Record Digital Photograph Optional	N/A	
Record Identifier	RMA Generated Paragraph C2.T3.1	
Content Management System	RMA captured Paragraph C2.T5.25.	Application used to manage files on the web.

C5.1.8.2.4. Mandatory Standard Record Elements. RMAs shall be able to export and import all record core mandatory metadata as well as the mandatory metadata in the following table.

Table C5.T9. Record (Transfer Mandatory)

Data Element	**Data Source**	**Content, Reference and Notes**
Record		
Record Identifier	RMA Generated Paragraph C2.T3.1	Unique record identifier
Supplemental Marking List	RMA captured Paragraph C2.T3.7	
Date Filed	RMA Generated Paragraph C2.T3.3	
Originating Organization	RMA captured Paragraph C2.T3.6	

C5.1.8.2.5. Defined-Optional Standard Record Elements. RMAs shall be able to export and import the defined optional metadata in the following table when this metadata is included in the RMA.

Table C5.T10. Record (Transfer Defined Optional)

Data Element	**Data Source**	**Content, Reference and Notes**
Record Defined		
Record Identifier	RMA Generated Paragraph C2.T3.1	Unique record identifier
Date Received	RMA captured Paragraph C2.T3.10	
Addressees	RMA captured Paragraph C2.T3.11	
Other Addressees	RMA captured Paragraph C2.T3.12	
Location	RMA captured Paragraph C2.T3.13	

C5.1.8.2.6. User Defined-Optional Record Elements. RMAs shall be able to export and import User-Defined Optional Record Elements

Table C5.T11. Record (Transfer User-Defined)

Data Element	**Data Source**	**Content, Reference and Notes**
Record User Defined	N/A	
Record Identifier	RMA Generated Paragraph C2.T3.1	Unique record identifier

Table C5.T11. Record (Transfer User-Defined)		
Data Element	**Data Source**	**Content, Reference and Notes**
Additional Information	As described in provider schema Paragraph C2.T3.14	Provider shall describe in extension schema

C5.1.8.3. Lifecycle Status Elements. RMAs shall capture and link additional life cycle metadata to records written out for bulk transfer. RMAs shall parse, ingest and link received record lifecycle information into the receiving database and/or repository.

C5.1.8.3.1. Lifecycle Status Elements. RMAs shall be able to export and import the mandatory lifecycle metadata in the following table.

Table C5.T12. Record Level Lifecycle (Transfer Mandatory)		
Data Element	**Data Source**	**Content, Reference and Notes**
Recordlifecycle		
Record Identifier	RMA Generated Paragraph C2.T3.1	Unique record identifier
Folder Identifier	RMA Generated Paragraph C2.T2.2	If folder is used
Record Category Identifier	RMA Generated Paragraph C2.T1.2	Link to the record category
Last Disposition Action	RMA Generated Paragraph C2.2.2.3	Lifecycle phase of the record
Last Disposition Action Date	RMA Generated Paragraph C2.2.2.3	Date the current phase started.
Final Disposition Action	RMA Generated Paragraph C2.2.2.3	From retention schedule of the associated record category
Final Disposition Date	RMA Generated Paragraph C2.2.2.3	Date final disposition action is to occur

C5.1.8.3.2. Record Level User-Defined Lifecycle Elements. RMAs shall be able to export and import any user-defined lifecycle metadata as intended in the following table.

Table C5.T13. Record Level Lifecycle (Transfer User-Defined)		
Data Element	**Data Source**	**Content, Reference and Notes**
RecordLifecycleUserDefined	N/A	
Record Identifier	RMA Generated Paragraph C2.T3.1	Unique record identifier
Additional Information	As described in provider schema Paragraph C2.T3.14	Provider shall describe in extension schema

C5.1.8.4. Record Folder Elements. When records are associated with folders, RMAs shall manage writing out record folders for bulk transfer with the metadata shown in the following paragraphs. RMAs shall parse and process all metadata elements during ingestion. Optionally RMAs shall provide authorized individuals with graphical user interface capabilities to support merging ingested folders into existing file plans.

C5.1.8.4.1. Record Folder Lifecycle Status Elements. RMAs shall capture and link additional life cycle metadata to record folders written out for bulk transfer. RMAs shall parse and ingest the record folder lifecycle information into the receiving RMA.

C5.1.8.4.2. Record Folder Level Mandatory Lifecycle Elements. RMAs shall be able to export and import all mandatory record folder lifecycle elements.

Table C5.T14. Folder Level (Defined Transfer Lifecycle Mandatory)

Data Element	**Data Source**	**Content, Reference and Notes**
FolderLifecycle		
Folder Identifier	RMA Generated Paragraph C2.T2.2	If folder is used
Record Category Identifier	RMA Generated Paragraph C2.T1.2	Link to the record category
Last Disposition Action	RME Generated Paragraph C2.2.2.3	Lifecycle phase of the folder
Last Disposition Action Date	RMA Generated Paragraph C2.2.2.3	Date the current phase started.
Final Disposition Action	RMA Generated Paragraph C2.2.2.3	From retention schedule of the associated record category
Final Disposition Date	RMA Generated Paragraph C2.2.2.3	Date final disposition action is to occur

C5.1.8.4.3. Record Folder Level User-Defined Lifecycle Elements. RMAs shall be able to export and import user-defined record folder lifecycle elements.

Table C5.T15. Folder Level Lifecycle (Transfer Lifecycle User-Defined)

Data Element	**Data Source**	**Content, Reference and Notes**
FolderLifecycleUserDefined	N/A	
Folder Identifier	RMA Generated Paragraph C2.T2.2	If folder is used
Additional Information	As described in provider schema Paragraph C2.T2.7	Provider shall describe in extension schema

C5.1.8.4.4. Standard Folder Elements. RMAs shall be able to export and import standard metadata to record folders written out for bulk transfer.

C5.1.8.4.5. Record Folder Level Mandatory Elements. RMAs shall be able to export and import mandatory record folder elements.

Table C5.T16. Folder Level (Transfer Mandatory)

Data Element	**Data Source**	**Content, Reference and Notes**
Folder		
Folder Identifier	RMA Generated Paragraph C2.T2.2	If folder is used
Record Category Identifier	RMA Generated Paragraph C2.T1.2	Link to the record category
Location	RMA captured Paragraph C2.T3.13	If location information is required
Vital Record Indicator	RMA captured Paragraph C2.T2.4	
Vital Record Review and Update Cycle Period	RMA captured Paragraph C2.T2.5	

C5.1.8.4.6. Record Folder Level Defined Optional Elements. RMAs shall be able to export and import defined optional record folder elements.

Table C5.T17. Folder Level (Transfer Defined Optional)

Data Element	**Data Source**	**Content, Reference and Notes**
FolderDefinedOptional		
Folder Identifier	RMA Generated Paragraph C2.T2.2	Link to folder
Supplemental Marking List	RMA captured Paragraph C2.T2.6	

C5.1.8.4.7. Record Folder Level User-Defined Elements. RMAs shall be able to export and import user-defined record folder elements.

Table C5.T18. Folder Level (Transfer User-Defined)

Data Element	**Data Source**	**Content, Reference and Notes**
Folder User Defined	N/A	
Folder Identifier	RMA Generated Paragraph C2.T2.2	Link to folder
Additional Information	As described in provider schema Paragraph C2.T2.7	Provider shall describe in extension schema

C5.1.9. Computer Files. The RMA shall be able to transfer and receive any type of computer files.

C5.1.9.1. Computer File Grouping. The RMA shall be able to group records according to the transfer schema and copy them to physical media to support archiving and transfer.

C5.1.9.2. Computer File Media Support. The RMA shall be able to read records from transfer media.

C5.1.9.3. Computer File Elements. RMAs shall associate Computer File elements with all record content, no matter the type or source.

Table C5.T19. Computer File Core (Defined Mandatory)

Data Element	**Data Source**	**Content, Reference and Notes**
Computer File	N/A	
Unique File ID	RMA Generated Paragraph C2.1.1	Unique identifier for this computer file.
File Name	Creating Applications or RMA captured	File name as stored on the media and may be accessible from the file properties.
File Extension	Creating Applications or RMA identified link Paragraph C2.1.1	Extension as stored on the media. The extension may be specific to an application, but that is not consistent. This information may be available from the file properties.
Creating Application	User entered specified or RMA identified link Paragraph C2.1.1	This is a pointer to the specific application that created this computer file. The information may be accessible from the file properties.
File Create Date	RMA and Operating System Paragraph C2.1.1	Date and time stamp for this file's creation. This information is available from the file properties, but may not be the original creation date of the record content.
File Size	RMA and Operating System Paragraph C2.1.1	Computer file size in bytes. (Need to verify that file size is consistent across operating systems that use different data block sizes.)
File Encoding	User Entered Paragraph C2.1.1	ASCII, UNICODE, EBCDIC, encryption standard, compression scheme, etc.
Specific Security	RMA Captured Paragraph C2.1.1	Optional. This covers internal security items such as sheet. protection, macros, PKI and digital signatures, and other features built into document formats.
Computer File	RMA and Operating System Paragraph C2.1.1	Binary content of the file. This data may be text or data associated with a specific application. The information is stored as binary on the media.

C5.2. SUPPORT OF SECURITY INTEROPERABILITY ELEMENTS

C5.2.1. The RMA shall write out and ingest security and/or protective marking information to each record exported from the repository.

C5.2.2. Security Markings. If Chapter 3 is implemented, the RMA shall write out and ingest security classification marking metadata to each record exported from the repository.

Table C5.T20. Security Marking Metadata

Data Element	**Data Source**	**Content, Reference and Notes**
SecurityClassification	N/A	Classification object or record
Current Classification	RMA Captured Paragraph C3.T1.2	One of Confidential, Secret, Top Secret, Unclassified
Initial Classification	RMA Captured Paragraph C3.T1.3	One of Confidential, Secret, Top Secret, Unclassified
Supplemental Marking	RMA Captured Paragraph C3.T1.7	List of agency provided informational or protective markings.

C5.2.3. Downgrading and Declassification. If Chapter 3 is implemented, the RMA shall write out and ingest downgrading and declassification metadata to each record exported from the repository.

Table C5.T21. Downgrading and Declassification Metadata

Data Element	**Data Source**	**Content, Reference and Notes**
Downgrading/Declassification Data	N/A	Downgrading/declassification object or record
Event	N/A	Text description of the event upon which information will be downgraded or declassified
Date	RMA Captured Paragraph C3.T1.14	Date upon which information will be downgraded or declassified
By	RMA Captured Paragraph C3.T1.13	Individual responsible for downgrading or declassifying information
Reason	RMA Captured Paragraph C3.T1.9	Text reason for downgrade or declassification
Type	N/A	One of Downgrade or Declassification

C5.3. OPTIONAL TRANSFER ELEMENTS

C5.3.1. File Plan Elements (Optional). RMAs should be able to export and import file plan components.

C5.3.1.1. Record Category Elements. RMAs should indicate whether disposition management is conducted at the folder or record level for each Record Category.

C5.3.1.1.1. Record Category Mandatory Elements. RMAs should be able to export and import mandatory record category elements.

Table C5.T22. Record Category (Defined Transfer Mandatory)

Data Element	**Data Source**	**Content, Reference and Notes**
RecordCategory		
Record Category Identifier	RMA Generated Paragraph C2.T1.2	Link to the record category
Record Category Name	RMA captured Paragraph C2.T1.1	Currently required by DoD 5015.2
Record Category Description	RMA captured Paragraph C2.T1.3	Currently required by DoD 5015.2
Disposition Authority	RMA captured Paragraph C2.T1.5	Currently required by DoD 5015.2
Permanent Record Indicator	RMA captured Paragraph C2.T1.6	Currently required by DoD 5015.2 as Transfer or Accession to NARA Indicator
Vital Record Indicator	RMA captured Paragraph C2.T1.7	Currently required by DoD 5015.2
Vital Record Review and Update Cycle Period	RMA captured Paragraph C2.T1.8	Currently required by DoD 5015.2
Disposition Level	RMA captured Paragraph C2.T1.4	One of Folder or Record

C5.3.1.2. Disposition Elements. RMAs should be able to export and import disposition components.

C5.3.1.2.1. Event Elements. RMAs should be able to export and import event metadata.

C5.3.1.2.2. Event Mandatory Elements. RMAs should be able to export and import mandatory event elements.

Table C5.T23. Events (Defined Transfer Mandatory)

Data Element	**Data Source**	**Content, Reference and Notes**
Event		
Event Identifier	RMA Generated Paragraph C2.2.2.8	Unique identifier for this event object.
Event Name	RMA captured Paragraph C2.2.2.8	Text description or name of event.

C5.3.1.2.3. Event User-Defined Elements. RMAs should be able to export and import user-defined event elements.

Table C5.T24. Events (Transfer User-Defined)

Data Element	**Data Source**	**Content, Reference and Notes**
EventUserDefined		

Table C5.T24. Events (Transfer User-Defined)		
Data Element	**Data Source**	**Content, Reference and Notes**
Event Identifier	RMA Generated Paragraph C2.2.2.8	Link to event.
Additional Information	As described in provider schema Paragraph C2.2.2.8	Provider should describe in extension schema.

C5.3.1.2.4. Trigger Elements. RMAs should be able to export and import disposition trigger metadata.

C5.3.1.2.5. Trigger Mandatory Elements. RMAs should be able to export and import mandatory trigger elements.

Table C5.T25. Trigger (Defined Transfer Mandatory)		
Data Element	**Data Source**	**Content, Reference and Notes**
Trigger		
Trigger Identifier	RMA captured Paragraph C2.2.2.4	Unique identifier for this trigger
Trigger type	RMA captured Paragraph C2.2.2.4	One of Cutoff, Vital Records Review, Interim Transfer
Trigger mode	RMA captured Paragraph C2.2.2.4	One of Event, Time, Time-Event
Event	RMA captured Paragraph C2.2.2.8	If Trigger mode is Event or Time-Event
Time Unit	RMA captured Paragraph C2.2.2.3	One of Daily, Weekly, Monthly, Quarterly, Semi-Annually, Annually
Time Unit Type	RMA captured Paragraph C2.2.2.3	One of Calendar, Fiscal
Time Unit Multiplier	RMA captured Paragraph C2.2.2.3	Number of time units used in calculations.
Trigger Execution Date	User-Entered or RMA Generated where Trigger Mode involves time calculation Paragraph C2.2.2.4	The calendar date the trigger is tripped.
Lifecycle Start Date	RMA Generated Paragraph C2.2.2.5	Retention start date based on trigger.

C5.3.1.2.6. Trigger User-Defined Elements. RMAs should be able to export and import user-defined trigger elements.

Table C5.T26. Trigger (Transfer User-Defined)		
Data Element	**Data Source**	**Content, Reference and Notes**
TriggerUserDefined		
Trigger Identifier	RMA Generated Paragraph C2.2.2.4	Unique identifier for this trigger
Additional Information	As described in provider schema Paragraph C2.2.2.4	Provider should describe in extension schema

C5.3.1.2.7. Vital Record Review Elements. RMAs should be able to export and import Vital Record Review metadata.

C5.3.1.2.8. Vital Record Review Mandatory Elements. RMAs should be able to export and import mandatory Vital Record Review elements.

Table C5.T27. Vital Record Review (Defined Transfer Mandatory)		
Data Element	**Data Source**	**Content, Reference and Notes**
Vital Record Review		
Vital Record Review Identifier	RMA Generated Paragraph C2.2.7.7.1	Unique identifier for this Vital Record Review
Vital Record Review type	RMA captured Paragraph C2.2.7.7.1	One of Cutoff, Vital Records Review, Interim Transfer
Vital Record Review mode	RMA captured Paragraph C2.2.7.7.1	One of Event, Time, Time-Event
Event	RMA captured Paragraph C2.2.2.8	If Vital Record Review mode is Event or Time-Event
Time Unit	User-Entered Paragraph C2.2.7.7.1	One of Daily, Weekly, Monthly, Quarterly, Semi-Annually, Annually
Time Unit Type	User-Entered Paragraph C2.2.7.7.1	One of Calendar, Fiscal
Time Unit Multiplier	User-Entered Paragraph C2.2.7.7.1	Number of time units used in calculations.
Vital Record Review Execution Date	User-Entered or RMA Generated where Vital Record Review Mode involves time calculation Paragraph C2.2.7.7.1	The calendar date the Vital Record Review is tripped.

C5.3.1.2.9. Vital Record Review User-Defined Elements. RMAs should be able to export and import user-defined Vital Record Review elements.

Table C5.T28. Vital Record Review (Transfer User-Defined)		
Data Element	**Data Source**	**Content, Reference and Notes**
Vital Record ReviewUserDefined		
Vital Record Review Identifier	RMA Generated Paragraph C2.2.7.7.1	Unique identifier for this Vital Record Review
Additional Information	As described in provider schema Paragraph C2.2.7.7.1	Provider should describe in extension schema

C5.3.1.2.10. Lifecycle Phase Elements. RMAs should be able to export and import lifecycle phase metadata.

C5.3.1.2.11. Lifecycle Phase Mandatory Elements. RMAs should be able to export and import mandatory lifecycle phase elements.

Table C5.T29. Lifecycle Phase (Defined Transfer Mandatory)		
Data Element	**Data Source**	**Content, Reference and Notes**
LifecyclePhase		
Lifecycle Phase Identifier	RMA Generated Paragraph C2.2.2.3	Unique identifier for this phase object
Lifecycle Phase Name	RMA captured Paragraph C2.2.2.3	Phase Name such as Records Holding Area, Current File Area, etc
Lifecycle Phase Precedence	RMA captured Paragraph C2.2.2.3	Order or precedence of this phase. Phases may share precedence.

C5.3.1.2.12. Lifecycle Phase User-Defined Elements. RMAs should be able to export and import user-defined lifecycle phase elements.

Table C5.T30. Lifecycle Phase (Transfer User-Defined)		
Data Element	**Data Source**	**Content, Reference and Notes**
Lifecycle Phase User Defined	NA	
Lifecycle Phase Identifier	RMA Generated Paragraph C2.2.2.3	If folder is used
Additional Information	As described in provider schema Paragraph C2.2.2.3	Provider should describe in extension schema

C5.4. ACCESS CONTROL.

C5.4.1. Table C5.T31. summarizes requirements that refer to "authorized individuals" and offers additional information regarding user-type responsibilities. In general, Application

Administrators are responsible for setting up the RMA infrastructure. Records Managers are responsible for records management administration. Privileged Users are those who are given special permissions to perform functions beyond those of typical users.

Table C5.T31. Authorized Individual Requirements

Requirement	**Application Administrator**	**Records Manager**	**Privileged User**
C5.1.4.2. Transfer Schema User-Defined … add to or remove from the schema user-defined, defined optional, and any vendor provided metadata fields.	During Set Up or At Export	At Export	NA
C5.1.5.2. Transfer Schema Metadata User-Defined Mapping … map metadata to schema elements to support export and ingest..	During Set Up or At Export/Import	At Export/ Import	NA
C5.1.6. User-Defined Elements Export Schemas and Rendering Aids … implement an export schema based on this standard and the vendor provided DTD. … remove the default if not needed by recipient.	During Set Up or At Export/Import	At Export/ Import	NA
C5.1.7. Record Elements … merging ingested records into existing file plans.	During Set Up or At Import	At Import	NA
C5.1.8.4 Record Folder Elements … merging ingested folders into existing file plans.	During Set Up or At Import	At Import	NA

C6. CHAPTER 6

NON-MANDATORY FEATURES

C6.1. REQUIREMENTS DEFINED BY THE ACQUIRING OR USING ACTIVITY

C6.1.1. In addition to the baseline requirements defined by this Standard, the acquiring or using activity should identify the following Agency-, site-, and installation-unique requirements. These requirements are not mandatory for DoD compliance.

C6.1.2. Storage Availability. The acquiring or using activity should define the size of the storage space required for its organizational records, along with the related record metadata and associated audit files.

C6.1.3. Documentation. The acquiring or using activity should determine the type and format of desired documentation, such as user guides, technical manuals, and installation procedures, to be provided by the vendor.

C6.1.4. System Performance. The acquiring or using activity should specify what constitutes acceptable RMA system availability, reliability, response times, and downtimes that will satisfy its business requirements.

C6.1.5. Hardware Environment. The acquiring or using activity should define the hardware environment (for example, mainframe, client-server, or personal computer) and identify the platforms (servers and workstations) on which the RMA is to run.

C6.1.6. Operating System Environment. The acquiring or using activity should define the operating system environment (for example, UNIX, Windows, Linux, Macintosh) on which the RMA is to be run.

C6.1.7. Network Environment. The acquiring or using activity should define the Local Area Network (LAN), Wide Area Network (WAN) or other network topology (e.g., Ethernet bus, star, or token-ring) and the Network Operating System (NOS) (e.g., Novell, Banyan Vines, Windows 2003 Server) on which the RMA is to be run.

C6.1.8. Protocols. The acquiring or using activity should identify the protocols, such as Transmission Control Protocol/Internet Protocol (TCP/IP), Simple Mail Transfer Protocol (SMTP), or X.400 that the RMA is to support.

C6.1.9. Electronic Mail Interface. The acquiring or using activity should specify the e-mail application(s) with which the RMA is to interface.

C6.1.10. End-User Orientation and Training. The acquiring or using activity should specify records manager and end-user training requirements.

C6.1.11. Harvesting Web Records. The acquiring or using activity should specify requirements necessary to meet NARA’s guidance on harvesting web content records. This includes links redirection, collection of script and business logic, and other archival management specific to web records.

C6.2. OTHER USEFUL RMA FEATURES

C6.2.1. Many RMA products provide the following time and laborsaving functions, either as standard or optional features to enhance the utility of the system (the acquiring or using activity should determine local requirements for any of the following RMA features).

C6.2.2. Making Global Changes. RMAs should provide the capability for authorized individuals to make global changes to the record category names, record category identifiers, disposition components, and originating organization. In addition, RMAs should provide the capability to reorganize the file plan and automatically propagate the changes resulting from the reorganization to the affected records and record folders.

C6.2.3. Bulk Loading Capability. RMAs should provide the capability for authorized individuals to bulk load:

C6.2.3.1. An Agency's pre-existing file plan.

C6.2.3.2. Electronic records.

C6.2.3.3. Record metadata.

C6.2.4. Interfaces to Other Software Applications. RMAs should interface with various office automation packages such as electronic mail, word processors, spreadsheets, databases, desktop publishers, web site harvesters, handheld devices, instant messengers, declassification review systems and electronic data interchange systems, as specified by the using activity.

C6.2.5. Report Writer Capability. RMAs should provide the capability to generate reports on the information held within the RMA’s repository based upon user-developed report templates or user queries.

C6.2.6. On-Line Help. RMAs should have an on-line help capability for access to user operational information. Help should be context sensitive to the screens from which help was launched. Global help should be available from a toolbar menu item or keyboard shortcut.

C6.2.7. Document Imaging Tools. RMAs should be capable of interfacing with document imaging and workflow software and hardware. These should be consistent with the DoD Automated Document Conversion Master Plan.

C6.2.8. Fax Integration Tools. An organization may determine a need for RMAs to interface with desktop or server-based fax products to capture fax records in their electronic format.

C6.2.9. Bar Code Systems. An organization may determine a need to use a bar code system with RMAs. The following examples show how bar code technology can be used to support records management tasks:

C6.2.9.1. File and correspondence tracking to positions, sections, or staff members.

C6.2.9.2. Creating, printing, and reading labels for non-electronic records.

C6.2.9.3. Boxing records for transfer.

C6.2.9.4. Box tracking for records-holding facility operations.

C6.2.9.5. Workflow tracking.

C6.2.9.6. Posting changes in disposition.

C6.2.9.7. Recording audit and census functions.

C6.2.10. Retrieval Assistance. RMAs should have additional search and retrieval features, such as full text search, to assist the user in locating records. The search utility should include the capability to create, modify, or import additional thesauri.

C6.2.11. File Plan Component Selection/Search Capability. RMAs should provide methods for assisting the user in the selection of the file plan components to be assigned to a record, such as priority-ordered lists or directed searches.

C6.2.12. Workflow and/or Document Management Features. An organization may determine that RMAs should have the capability to manage working and draft versions of documents and other potential record materials as they are being developed.

C6.2.13. Records Management Forms and Other Forms. An organization may determine that RMAs should be capable of interfacing with forms generating software and/or have the capability to generate completed standard records management forms, such as:

C6.2.13.1. Standard Forms 115 and 115-A, "Request for Records Disposition Authority."

C6.2.13.2. Standard Forms 135 and 135-A, "Records Transmittal and Receipt."

C6.2.13.3. Standard Form 258, "Agreement To Transfer Records To The National Archives Of The United States."

C6.2.13.4. National Archives Form 14012, "Database Record Layout."

C6.2.13.5. National Archives Form 14097, "Technical Description for Transfer of Electronic Records to the National Archives."

C6.2.14. Printed Labels. RMAs should provide the capability to produce hard-copy codes or identifiers in the form of labels or other products, as required.

C6.2.15. Viewer. RMAs should provide the capability to view each file in its stored format or a human-readable rendition.

C6.2.16. Web Capability. RMAs should provide the capability to allow the user to interface through a web browser or other platform independent means.

C6.2.17. Government Information Locator Service. RMAs should have the capability to implement the requirements of the Government Information Locator Service (GILS) (see reference (n)). GILS was established to identify public information resources throughout the Federal Government, describe the information available in those resources, and provide assistance in obtaining this information.

C6.2.18. Enhanced Support for Off-line Records. RMAs should provide additional features for managing boxes of hard copy records and other off-line archives.

C6.2.19. Organizational Customization**.**

C6.2.19.1. Data Entry Screens. RMAs should provide the capability for authorized individuals to arrange record metadata components and user-defined record components on data entry screens to be used for filing.

C6.2.19.2. Default Metadata Values. RMAs should provide the capability for authorized individuals to assign default values to record metadata components and user-defined record components that will be shown data entry screens to be used for filing.

C6.2.19.3. User Picklists. RMAs shall provide the capability for users to create and maintain shortened "quick–pick" lists from the authorized lists.

C6.2.19.4. User Templates. RMAs shall provide the capability for users to create and maintain templates that automatically populate commonly used data into record metadata fields.

C6.3. SEARCH AND DISCOVERY INTEROPERABILITY

C6.3.1. RMAs should make designated records available for public search and retrieval and optionally support e-FOIA/e-Privacy Act requests.

C6.3.2. Service-Oriented Discovery. RMAs should provide graphical user interface capabilities to allow authorized individuals to make holdings available via a service-oriented architecture. RMA implementation should support compliance with the Global Information Grid's Service Oriented Architecture policies (see UDDI, IM Strategic Plan, C4ISR Architecture, GIG Architecture, GIG Capstone Requirements, and DISR., references (aw), (ax), (ay), (az), (ba), and (bb)).

C6.3.2.1. Holdings Announcement. RMAs should provide graphical user interface capabilities to allow authorized individuals to create/update and publish a holdings announcement to the enterprise services registry. Such a holdings announcement should include DDMS-formatted (reference (c)) metadata, in order to provide visibility for holdings compliant with DoDD 8320.2 (reference (bc), (bd)). RMAs shall provide graphical user interface capabilities to allow authorized individuals to create and publish a removal of services announcement to the enterprise services registry.

C6.3.2.2. Service Connection Instructions. RMAs should provide graphical user interface capabilities to allow authorized individuals to create/update and publish service connection instructions to the enterprise services registry.

C6.3.2.3. Service Requests and Queries. RMAs should make their holdings accessible to the Enterprise, conforming to DoDD 8320.2 (reference (bc), (bd)) by responding to service requests and queries that are composed in accordance with the published service connection instructions. RMAs should include the capability to provide access to record metadata visible to both known and authorized unanticipated users in the DoD enterprise. Additionally, RMAs should include the capability to make web-enabled records management business and computing processes visible to the DoD enterprise.

C6.4. ACCESS CONTROL.

C6.4.1. Table C6.T1. summarizes requirements that refer to "authorized individuals" and offers additional information regarding user-type responsibilities. In general, Application Administrators are responsible for setting up the RMA infrastructure. Records Managers are responsible for records management administration. Privileged Users are those who are given special permissions to perform functions beyond those of typical users.

Table C6.T1. Authorized Individual Requirements

Requirement	**Application Administrator**	**Records Manager**	**Privileged User**
C6.2.2. Making Global Changes. … make global changes to the record category names, record category identifiers, disposition components, and originating organization. … reorganize the file plan and automatically propagate the changes .	Optional Access As Needed	As Needed	Permitted portions of file plan only
C6.2.3. Bulk Loading Capability. RMAs should provide the capability for authorized individuals to bulk load:	Optional Access As Needed	As Needed	NA
C6.2.19.1. Data Entry Screens. … arrange record metadata components and user-defined record components on data entry screens to be used for filing.	During Set up	As Needed	NA
C6.2.18,2. Default Metadata Values. … assign default values to record metadata components and user-defined record components …	During Set up	As Needed	NA
C6.3.2. Service Oriented Discovery. … allow authorized individuals to make holdings available via a service oriented architecture.	Optional Access As Needed	As Needed	NA
C6.3.2.1. Holdings Announcement. … create/update and publish a holdings announcement to the enterprise services registry. …create and publish a removal of services announcement to the enterprise services registry.	Optional Access As Needed	As Needed	NA
C6.3.2.2. Service Connection Instructions. … create/update and publish service connection instructions to the enterprise services registry.	Optional Access As Needed	As Needed	NA

(This page intentionally left blank.)

APPENDIX A.

Mandatory Transfer Schemas

RMAs shall be able to write out records and record folders using the following XML schemas.

RMAs shall be able to read in and ingest records using the following XML schemas.

Computer File Schema

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:add="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/AdditionalInfo
rmation"
xmlns:cf="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/ComputerFile"
targetNamespace="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/Computer
File" elementFormDefault="qualified">
<xs:import
namespace="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/AdditionalInfo
rmation" schemaLocation="AdditionalInformation.xsd"/>
<xs:element name="ComputerFile" type="cf:ComputerFile"/>
      <xs:complexType name="ComputerFile">
            <xs:sequence>
                  <xs:element name="ComputerFileBinary" type="xs:string"/>
                  <xs:element ref="cf:ComputerFileUserDefined"/>
            </xs:sequence>
            <xs:attributeGroup ref="cf:ComputerFileAtt"/>
      </xs:complexType>
      <xs:attributeGroup name="ComputerFileAtt">
            <xs:attribute name="UniqueFileId" type="xs:string"
use="required"/>
            <xs:attribute name="FileName" type="xs:string" use="required"/>
            <xs:attribute name="FileExtension" type="xs:string"
use="required"/>
            <xs:attribute name="CreatingApplication" type="xs:string"
use="required"/>
            <xs:attribute name="FileCreateDate" type="xs:date"
use="required"/>
            <xs:attribute name="FileSize" type="xs:int" use="required"/>
            <xs:attribute name="FileEncoding" type="xs:string"
use="required"/>
            <xs:attribute name="SpecificSecurity" type="xs:string"
use="optional"/>
      </xs:attributeGroup>
      <xs:element name="ComputerFileUserDefined"
type="cf:ComputerFileUserDefined"/>
      <xs:complexType name="ComputerFileUserDefined">
            <xs:sequence>
                  <xs:element name="PCData" type="xs:string"/>
                  <xs:element ref="add:AdditionalInformation"/>
                  <xs:any minOccurs="0" maxOccurs="unbounded"
processContents="lax"/>
            </xs:sequence>
            <xs:attributeGroup ref="cf:ComputerFileUserDefinedAtt"/>
      </xs:complexType>
      <xs:attributeGroup name="ComputerFileUserDefinedAtt">
            <xs:attribute name="UniqueFileID" type="xs:string"
use="required"/>
```

```
      </xs:attributeGroup>
</xs:schema>
```

Record Mandatory Schema

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:add="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/AdditionalInfo
rmation"
xmlns:rec="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/Record"
xmlns:sm="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/SecurityMarking
"
xmlns:nslc="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/RecordLifeCyc
le"
xmlns:nscf="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/ComputerFile"
targetNamespace="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/Record"
elementFormDefault="qualified">
      <xs:import
namespace="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/ComputerFile"
schemaLocation="ComputerFile.xsd"/>
      <xs:import
namespace="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/RecordLifeCycl
e" schemaLocation="RecordLifeCycle.xsd"/>
      <xs:import
namespace="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/SecurityMarkin
g" schemaLocation="SecurityMarking.xsd"/>
      <xs:import
namespace="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/AdditionalInfo
rmation" schemaLocation="AdditionalInformation.xsd"/>
      <xs:element name="Record" type="rec:Record"/>
      <xs:complexType name="Record">
            <xs:sequence>
                  <xs:element name="SupportingFilesLink">
                   <xs:complexType>
                        <xs:sequence>
                          <xs:element name="RecordIdentifier"
type="xs:string" minOccurs="0" maxOccurs="unbounded"/>
                          <xs:element name="FolderIdentifier"
type="xs:string" minOccurs="0" maxOccurs="unbounded"/>
                        </xs:sequence>
                    </xs:complexType>
                   </xs:element>
                   <xs:element name="OriginalContent">
                        <xs:complexType>
                              <xs:sequence>
                                    <xs:element ref="nscf:ComputerFile"/>
                              </xs:sequence>
                        </xs:complexType>
                  </xs:element>
                  <xs:element name="OpenContent">
                        <xs:complexType>
                              <xs:sequence>
                                    <xs:element ref="nscf:ComputerFile"/>
                              </xs:sequence>
                        </xs:complexType>
                  </xs:element>
                  <xs:element name="RecordLifeCycle">
                        <xs:complexType>
                              <xs:sequence>
                                    <xs:element ref="nslc:RecordLifeCycle"/>
                              </xs:sequence>
                        </xs:complexType>
                  </xs:element>
                  <xs:element name="SecurityMarking" minOccurs="0" >
                        <xs:complexType>
                              <xs:sequence>
                                    <xs:element ref="sm:SecurityMarking"/>
                              </xs:sequence>
                        </xs:complexType>
                  </xs:element>
            <xs:element name="SupplementalMarkingList" type="xs:string"
minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="OriginatingOrganization" type="xs:string"/>
            <xs:element ref="rec:RecordUserDefined"/>
            </xs:sequence>
            <xs:attributeGroup ref="rec:RecordAtt"/>
      </xs:complexType>
      <xs:attributeGroup name="RecordAtt">
            <xs:attribute name="RecordIdentifier" type="xs:string"
use="required"/>
            <xs:attribute name="FolderIdentifier" type="xs:string"
use="required"/>
            <xs:attribute name="Title" type="xs:string" use="required"/>
            <xs:attribute name="Author" type="xs:string" use="required"/>
            <xs:attribute name="Media" type="xs:string" use="required"/>
            <xs:attribute name="Format" type="xs:string" use="required"/>
            <xs:attribute name="DateFiled" type="xs:string" use="required"/>
            <xs:attribute name="DatePublished" type="xs:string"
use="required"/>
            <xs:attribute name="DateReceived" type="xs:string"
use="optional"/>
            <xs:attribute name="Addressees" type="xs:string" use="optional"/>
            <xs:attribute name="OtherAddressees" type="xs:string"
use="optional"/>
            <xs:attribute name="Location" type="xs:string" use="optional"/>
            </xs:attributeGroup>
            <xs:element name="RecordUserDefined"
type="rec:RecordUserDefined"/>
            <xs:complexType name="RecordUserDefined">
            <xs:sequence>
                  <xs:element ref="add:AdditionalInformation"/>
                  <xs:any minOccurs="0" maxOccurs="unbounded"
processContents="lax"/>
```

```
            </xs:sequence>
            <xs:attributeGroup ref="rec:RecordUserDefinedAtt"/>
      </xs:complexType>
      <xs:attributeGroup name="RecordUserDefinedAtt">
            <xs:attribute name="RecordIdentifier" type="xs:string"
use="required"/>
            </xs:attributeGroup>
      <!-- end of record element and its attributes-->
      <xs:element name="RecordEmail" type="rec:RecordEmail"/>
      <xs:complexType name="RecordEmail">
            <xs:sequence>
                  <xs:element name="Record">
                        <xs:complexType>
                              <xs:sequence>
                                    <xs:element ref="rec:Record"/>
                              </xs:sequence>
                        </xs:complexType>
                  </xs:element>
                  <xs:element name="AttachmentReference">
                        <xs:complexType>
                        <xs:sequence>
                          <xs:element name="RecordIdentifier"
type="xs:string" minOccurs="0" maxOccurs="unbounded"/>
                          <xs:element name="FolderIdentifier"
type="xs:string" minOccurs="0" maxOccurs="unbounded"/>
                        </xs:sequence>
                    </xs:complexType>
                  </xs:element>
            </xs:sequence>
            <xs:attributeGroup ref="rec:RecordEmailAtt"/>
      </xs:complexType>
      <xs:attributeGroup name="RecordEmailAtt">
            <xs:attribute name="RecordIdentifier" type="xs:string"
use="required"/>
            <xs:attribute name="Sender" type="xs:string" use="required"/>
            <xs:attribute name="PrimaryAddress" type="xs:string"
use="required"/>
            <xs:attribute name="SecondaryAddress" type="xs:string"
use="optional"/>
            <xs:attribute name="HiddenAddress" type="xs:string"
use="optional"/>
            <xs:attribute name="EmailSubject" type="xs:string"
use="required"/>
            <xs:attribute name="SentTimestamp" type="xs:string"
use="required"/>
            <xs:attribute name="ReceivedTimestamp" type="xs:string"
use="optional"/>
      </xs:attributeGroup>
      <xs:element name="RecordScanned" type="rec:RecordScanned"/>
      <xs:complexType name="RecordScanned">
```

```
            <xs:sequence>
                  <xs:element name="Record">
                        <xs:complexType>
                              <xs:sequence>
                                    <xs:element ref="rec:Record"/>
                              </xs:sequence>
                        </xs:complexType>
                  </xs:element>
            </xs:sequence>
            </xs:complexType>
      <xs:attributeGroup name="RecordScannedAtt">
            <xs:attribute name="RecordIdentifier" type="xs:string"
use="required"/>
            <xs:attribute name="ImageResolution" type="xs:string"
use="required"/>
            <xs:attribute name="ScannedImageFormatAndVersion"
type="xs:string" use="required"/>
            <xs:attribute name="ImageBitDepth" type="xs:string"
use="optional"/>
      </xs:attributeGroup>
      <xs:element name="RecordPDF" type="rec:RecordPDF"/>
      <xs:complexType name="RecordPDF">
            <xs:sequence>
                  <xs:element name="Record">
                        <xs:complexType>
                              <xs:sequence>
                                    <xs:element ref="rec:Record"/>
                              </xs:sequence>
                        </xs:complexType>
                  </xs:element>
                  </xs:sequence>
            <xs:attributeGroup ref="rec:RecordPDFAtt"/>
      </xs:complexType>
      <xs:attributeGroup name="RecordPDFAtt">
            <xs:attribute name="RecordIdentifier" type="xs:string"
use="required"/>
            <xs:attribute name="ProducingApplication" type="xs:string"
use="required"/>
            <xs:attribute name="ProducingApplicationVersion" type="xs:string"
use="required"/>
            <xs:attribute name="PDFVersion" type="xs:string" use="required"/>
            <xs:attribute name="CreatingApplication" type="xs:string"
use="optional"/>
            <xs:attribute name="DocumentSecuritySetting" type="xs:string"
use="optional"/>
      </xs:attributeGroup>
      <xs:element name="RecordDigitalPhotograph"
type="rec:RecordDigitalPhotograph"/>
      <xs:complexType name="RecordDigitalPhotograph">
            <xs:sequence>
```

```
                  <xs:element name="Record">
                        <xs:complexType>
                              <xs:sequence>
                                    <xs:element ref="rec:Record"/>
                              </xs:sequence>
                        </xs:complexType>
                  </xs:element>
              </xs:sequence>
            <xs:attributeGroup ref="rec:RecordDigitalPhotographAtt"/>
      </xs:complexType>
      <xs:attributeGroup name="RecordDigitalPhotographAtt">
            <xs:attribute name="RecordIdentifier" type="xs:string"
use="required"/>
            <xs:attribute name="Caption" type="xs:string" use="required"/>
            <xs:attribute name="Photographer" type="xs:string"
use="optional"/>
            <xs:attribute name="CopyRight" type="xs:string" use="optional"/>
            <xs:attribute name="BitDepth" type="xs:string" use="required"/>
            <xs:attribute name="ImageSize" type="xs:string" use="optional"/>
            <xs:attribute name="ImageSource" type="xs:string"
use="optional"/>
            <xs:attribute name="Compression" type="xs:string"
use="optional"/>
            <xs:attribute name="ICCMProfile" type="xs:string"
use="optional"/>
            <xs:attribute name="EXIFInformation" type="xs:string"
use="optional"/>
      </xs:attributeGroup>
      <xs:element name="RecordWeb" type="rec:RecordWeb"/>
      <xs:complexType name="RecordWeb">
            <xs:sequence>
                  <xs:element name="Record">
                        <xs:complexType>
                              <xs:sequence>
                                    <xs:element ref="rec:Record"/>
                              </xs:sequence>
                        </xs:complexType>
                  </xs:element>
                  <xs:element name="Contact" type="xs:string"/>
                    </xs:sequence>
            <xs:attributeGroup ref="rec:RecordWebAtt"/>
      </xs:complexType>
      <xs:attributeGroup name="RecordWebAtt">
            <xs:attribute name="RecordIdentifier" type="xs:string"
use="required"/>
            <xs:attribute name="FileName" type="xs:string" use="required"/>
            <xs:attribute name="WebPlatform" type="xs:string"
use="required"/>
            <xs:attribute name="WebSiteName" type="xs:string"
use="required"/>
```

```
            <xs:attribute name="WebSiteURL" type="xs:string" use="required"/>
            <xs:attribute name="CaptureMethod" type="xs:string"
use="required"/>
            <xs:attribute name="CaptureDate" type="xs:string"
use="required"/>
            <xs:attribute name="ContentManagementSystem" type="xs:string"
use="optional"/>
      </xs:attributeGroup>
 </xs:schema>
```

Record Life Cycle Schema

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:rlc="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/RecordLifeCycl
e"
targetNamespace="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/RecordLi
feCycle" elementFormDefault="qualified">
      <xs:element name="RecordLifeCycle" type="rlc:RecordLifeCycle"/>
      <xs:complexType name="RecordLifeCycle">
            <xs:sequence>
                  <xs:element name="LastDispostionActionDate"
type="xs:string"/>
                  <xs:element name="FinalDispositionActionDate"
type="xs:string"/>
                  <xs:element name="LastDispostionAction" type="xs:string"/>
                  <xs:element name="FinalDispositionAction">
                  <xs:simpleType>
                    <xs:restriction base="xs:string">
                        <xs:enumeration value="Permanent"/>
                        <xs:enumeration value="Destroyed"/>
                     </xs:restriction>
                     </xs:simpleType></xs:element>
                  <xs:element name="RecordLifeCycleUserDefined">
                        <xs:complexType>
                              <xs:sequence>
                                    <xs:element
ref="rlc:RecordLifeCycleUserDefined"/>
                              </xs:sequence>
                        </xs:complexType>
                  </xs:element>
            </xs:sequence>
            <xs:attributeGroup ref="rlc:RecordLifeCycleAtt"/>
      </xs:complexType>
      <xs:attributeGroup name="RecordLifeCycleAtt">
            <xs:attribute name="RecordIdentifier" type="xs:string"
use="required"/>
            <xs:attribute name="FolderIdentifier" type="xs:string"
use="optional"/>
            <xs:attribute name="RecordCategoryIdentifier" type="xs:string"
use="required"/>
      </xs:attributeGroup>
      <xs:element name="RecordLifeCycleUserDefined"
type="rlc:RecordLifeCycleUserDefined"/>
      <xs:complexType name="RecordLifeCycleUserDefined">
            <xs:sequence>
                  <xs:element name="AdditionalIformation" type="xs:string"/>
                  <xs:any minOccurs="0" maxOccurs="unbounded"
processContents="lax"/>
            </xs:sequence>
            <xs:attributeGroup ref="rlc:RecordLifeCycleUserDefinedAtt"/>
      </xs:complexType>
      <xs:attributeGroup name="RecordLifeCycleUserDefinedAtt">
            <xs:attribute name="RecordIdentifier" type="xs:string"
use="required"/>
            <xs:anyAttribute processContents="lax"/>
      </xs:attributeGroup>
</xs:schema>
```

Folder Schema

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:ns2="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/FolderLifeCycl
e"
xmlns:add="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/AdditionalInfo
rmation"
xmlns:fol="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/Folder"
targetNamespace="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/Folder"
elementFormDefault="qualified">
      <xs:import
namespace="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/FolderLifeCycl
e" schemaLocation="FolderLifeCycle.xsd"/>
      <xs:import
namespace="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/AdditionalInfo
rmation" schemaLocation="AdditionalInformation.xsd"/>
      <xs:element name="Folder" type="fol:Folder"/>
      <xs:complexType name="Folder">
            <xs:sequence>
                  <xs:element name="VitalRecordReviewandUpdateCyclePeriod"
type="xs:int"/>
                  <xs:element name="SupplementalMarkingList" type="xs:string"
minOccurs="0" maxOccurs="unbounded"/>
                  <xs:element name="FolderLifeCycle">
                   <xs:complexType>
                              <xs:sequence>
                                    <xs:element ref="ns2:FolderLifeCycle"
minOccurs="1"/>
                              </xs:sequence>
                        </xs:complexType>
                   </xs:element>
                   <xs:element ref="fol:FolderUserDefined"/>
             </xs:sequence>
            <xs:attributeGroup ref="fol:FolderAtt"/>
      </xs:complexType>
      <xs:attributeGroup name="FolderAtt">
            <xs:attribute name="FolderName" type="xs:string" use="required"/>
            <xs:attribute name="FolderIdentifier" type="xs:string"
use="required"/>
            <xs:attribute name="RecordCategoryIdentifier" type="xs:string"
use="required"/>
            <xs:attribute name="Location" type="xs:string" use="optional"/>
            <xs:attribute name="VitalRecordIndictor" type="xs:boolean"
use="required"/>
            </xs:attributeGroup>
      <xs:element name="FolderUserDefined">
            <xs:complexType>
            <xs:sequence>
                  <xs:element ref="add:AdditionalInformation"/>
                  <xs:any processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
            </xs:sequence>
            <xs:attributeGroup ref="fol:FolderUserDefinedAtt"/>
      </xs:complexType>
      </xs:element>
      <xs:attributeGroup name="FolderUserDefinedAtt">
            <xs:attribute name="FolderIdentifier" type="xs:string"
use="required"/>
            </xs:attributeGroup>
</xs:schema>
```

Folder Lifecycle Schema

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:add="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/AdditionalInfo
rmation"
xmlns:ns1="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/FolderLifeCycl
e"
targetNamespace="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/FolderLi
feCycle" elementFormDefault="qualified">
<xs:import
namespace="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/AdditionalInfo
rmation" schemaLocation="AdditionalInformation.xsd"/>
      <xs:element name="FolderLifeCycle" type="ns1:FolderLifeCycle"/>
      <xs:complexType name="FolderLifeCycle">
            <xs:sequence>
                  <xs:element name="LastDispostionActionDate"
type="xs:string"/>
                  <xs:element name="FinalDispositionActionDate"
type="xs:string"/>
                  <xs:element name="LastDispostionAction" type="xs:string"/>
                  <xs:element name="FinalDispositionAction">
                   <xs:complexType>
                        <xs:choice>
                              <xs:element name="Permanent" type="xs:string"/>
                              <xs:element name="Destroyed" type="xs:string"/>
                           </xs:choice>
                        </xs:complexType>
                        </xs:element>
                   <xs:element ref="ns1:FolderLifecycleUserDefined"/>
              </xs:sequence>
            <xs:attributeGroup ref="ns1:FolderLifeCycleAtt"/>
      </xs:complexType>
      <xs:attributeGroup name="FolderLifeCycleAtt">
            <xs:attribute name="FolderIdentifier" type="xs:string"
use="required"/>
            <xs:attribute name="RecordCategoryIdentifier" type="xs:string"
use="required"/>
            </xs:attributeGroup>
      <xs:element name="FolderLifecycleUserDefined"/>
      <xs:complexType name="FolderLifecycleUserDefined">
            <xs:sequence>
                  <xs:element ref="add:AdditionalInformation"/>
                  <xs:any minOccurs="0" maxOccurs="unbounded"
processContents="lax"/>
            </xs:sequence>
            <xs:attributeGroup ref="ns1:FolderLifecycleUserDefinedAtt"/>
      </xs:complexType>
      <xs:attributeGroup name="FolderLifecycleUserDefinedAtt">
            <xs:attribute name="FolderIdentifier" type="xs:string"/>
```

```
    </xs:attributeGroup>
</xs:schema>
```

Security Marking Schema

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:rsm="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/SecurityMarkin
g"
targetNamespace="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/Security
Marking" elementFormDefault="qualified">
<xs:element name="SecurityMarking" type="rsm:SecurityMarking"/>
      <xs:complexType name="SecurityMarking">
            <xs:sequence>
            <xs:element name="SecurityClassification">
                  <xs:complexType>
                        <xs:sequence>
                              <xs:element ref="rsm:SecurityClassification"/>
                        </xs:sequence>
                  </xs:complexType>
            </xs:element>
            <xs:element name="DowngradingDeclassification">
                  <xs:complexType>
                        <xs:sequence>
                                    <xs:element
ref="rsm:DowngradingDeclassification"/>
                        </xs:sequence>
                  </xs:complexType>
            </xs:element>
            </xs:sequence>
      <xs:attributeGroup ref="rsm:SecurityMarkingAtt"/>
      </xs:complexType>
      <xs:attributeGroup name="SecurityMarkingAtt">
            <xs:attribute name="RecordIdentifier" type="xs:string"
use="required"/>
      </xs:attributeGroup>
      <xs:element name="SecurityClassification"
type="rsm:SecurityClassification"/>
      <xs:complexType name="SecurityClassification">
            <xs:sequence>
                  <xs:element name="CurrentClassification">
                   <xs:complexType>
                        <xs:choice>
                           <xs:element name="Confidential" type="xs:string"/>
                           <xs:element name="Secret" type="xs:string"/>
                           <xs:element name="TopSecret" type="xs:string"/>
                         </xs:choice>
                        </xs:complexType>
                    </xs:element>
                   <xs:element name="InitialClassification">
                      <xs:complexType>
                         <xs:choice>
```

```
                            <xs:element name="Confidential"
type="xs:string"/>
                              <xs:element name="Secret" type="xs:string"/>
                            <xs:element name="TopSecret" type="xs:string"/>
                           </xs:choice>
                           </xs:complexType>
                        </xs:element>
                  <xs:element name="SupplementalMarkingList" type="xs:string"
minOccurs="0" maxOccurs="unbounded"/>
            </xs:sequence>
         </xs:complexType>
      <xs:element name="DowngradingDeclassification"
type="rsm:DowngradingDeclassification"/>
      <xs:complexType name="DowngradingDeclassification">
            <xs:sequence>
                  <xs:element name="EventDescription" type="xs:string"/>
                  <xs:element name="Date" type="xs:date"/>
                  <xs:element name="Type">
                    <xs:complexType>
                        <xs:choice>
                              <xs:element name="Downgrade" type="xs:string"/>
                           <xs:element name="Declassification"
type="xs:string"/>
                        </xs:choice>
                        </xs:complexType>
                  </xs:element>
            </xs:sequence>
            <xs:attributeGroup ref="rsm:DowngradingDeclassificationAtt"/>
      </xs:complexType>
      <xs:attributeGroup name="DowngradingDeclassificationAtt">
            <xs:attribute name="By" type="xs:string" use="required"/>
            <xs:attribute name="Reason" type="xs:string" use="required"/>
      </xs:attributeGroup>
</xs:schema>
```

Additional Information Schema

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:add="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/AdditionalInfo
rmation"
targetNamespace="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/Addition
alInformation" elementFormDefault="qualified">
<xsd:element name="AdditionalInformation">
      <xsd:complexType>
            <xsd:sequence>
                  <xsd:any minOccurs="1" maxOccurs="unbounded"
processContents="lax"/>
            </xsd:sequence>
            <xsd:anyAttribute processContents="lax"/>
       </xsd:complexType>
      </xsd:element>
</xsd:schema>
```

APPENDIX B

Optional Transfer Schemas

RMAs should be able to write out records and record folders using the following XML schemas.

RMAs should be able to read in and ingest records using the following XML schemas.

Record Category Schema

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:dis="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/Disposition"
xmlns:rcat="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/RecordCategor
y"
targetNamespace="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/RecordCa
tegory" elementFormDefault="qualified">
<xs:import
namespace="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/Disposition"
schemaLocation="Disposition.xsd"/>
      <xs:element name="RecordCategory" type="rcat:RecordCategory"/>
      <xs:complexType name="RecordCategory">
            <xs:sequence>
                  <xs:element name="VitalRecordReviewAndUpdateCyclePeriod"
type="xs:int"/>
                  <xs:element name="Disposition">
                   <xs:complexType>
                        <xs:sequence>
                          <xs:element ref="dis:Disposition"/>
                        </xs:sequence>
                        </xs:complexType>
                  </xs:element>
                  <xs:element name="DispositionLevel">
                  <xs:simpleType>
                   <xs:restriction base="xs:string">
                   <xs:enumeration value="Record"/>
                   <xs:enumeration value="Folder"/>
                   </xs:restriction>
             </xs:simpleType>
                   </xs:element>
                   <xs:element name="PermanentRecordIndicator">
               <xs:simpleType >
                      <xs:restriction base="xs:string">
                         <xs:enumeration value="Transfer"/>
                         <xs:enumeration value="Accession"/>
                        </xs:restriction>
                      </xs:simpleType>
                        </xs:element>
                    <xs:element ref="dis:Disposition"/>
                   </xs:sequence>
            <xs:attributeGroup ref="rcat:RecordCategoryAtt"/>
      </xs:complexType>
      <xs:attributeGroup name="RecordCategoryAtt">
            <xs:attribute name="RecordCategoryIdentifier" type="xs:string"
use="required" />
            <xs:attribute name="RecordCategoryName" type="xs:string"
use="required"/>
```

```
            <xs:attribute name="RecordCategoryDescription" type="xs:string"
use="required"/>
            <xs:attribute name="DispositionAuthority" type="xs:string"
use="required"/>
            <xs:attribute name="VitalRecordIndicator" type="xs:boolean"
use="required"/>
            </xs:attributeGroup>
      </xs:schema>
```

Disposition Schema

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:add="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/AdditionalInfo
rmation"
xmlns:dis="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/Disposition"
targetNamespace="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/Disposit
ion" elementFormDefault="qualified">
<xs:import
namespace="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/AdditionalInfo
rmation" schemaLocation="AdditionalInformation.xsd"/>

      <xs:element name="Disposition" type="dis:Disposition"/>
      <xs:complexType name="Disposition">
      <xs:sequence>
            <xs:element name="Trigger">
              <xs:complexType>
                  <xs:sequence>
                        <xs:element ref="dis:Trigger"/>
                        </xs:sequence>
                  </xs:complexType>
              </xs:element>
              <xs:element name="Event">
              <xs:complexType>
                <xs:sequence>
                        <xs:element ref="dis:Event"/>
                  </xs:sequence>
              </xs:complexType>
            </xs:element>
         </xs:sequence>
        </xs:complexType>
        <xs:element name="Trigger" type="dis:Trigger"/>
             <xs:complexType name="Trigger">
              <xs:sequence>
                  <xs:element name="TriggerType">
                   <xs:complexType>
                        <xs:choice>
                           <xs:element name="Cutoff" type="xs:string"/>
                           <xs:element name="VitalRecordsReview"
type="xs:string"/>
                           <xs:element name="InterimTransfer"
type="xs:string"/>
                        </xs:choice>
                        </xs:complexType>
                        </xs:element>
                  <xs:element name="TriggerMode">
                   <xs:complexType>
                        <xs:choice>
                              <xs:element name="Time" type="xs:string"/>
                        <xs:element name="Event" type="xs:string"/>
                        <xs:element name="TimeEvent" type="xs:string"/>
                         </xs:choice>
                        </xs:complexType>
                  </xs:element>
                  <xs:element name="Event">
                  <xs:complexType>
                        <xs:sequence>
                              <xs:element ref="dis:Event"/>
                         </xs:sequence>
                  </xs:complexType>
                  </xs:element>
                  <xs:element name="TimeUnit">
                    <xs:complexType>
                        <xs:choice>
                              <xs:element name="Daily" type="xs:string"/>
                              <xs:element name="Weekly" type="xs:string"/>
                              <xs:element name="Monthly" type="xs:string"/>
                              <xs:element name="Quarterly" type="xs:string"/>
                              <xs:element name="SemiAnnually"
type="xs:string"/>
                              <xs:element name="Annually" type="xs:string"/>
                           </xs:choice>
                        </xs:complexType>
                  </xs:element>
                  <xs:element name="TimeUnitType">
                   <xs:complexType>
                        <xs:choice>
                              <xs:element name="Fiscal" type="xs:string"/>
                              <xs:element name="Calendar" type="xs:string"/>
                         </xs:choice>
                         </xs:complexType>
                  </xs:element>
                  <xs:element name="TriggerUserDefined">
                        <xs:complexType>
                              <xs:sequence>
                              <xs:element ref="dis:TriggerUserDefined"/>
                        </xs:sequence>
                  </xs:complexType>
            </xs:element>
            </xs:sequence>
         <xs:attributeGroup ref="dis:TriggerAtt"/>
      </xs:complexType>
      <xs:attributeGroup name="TriggerAtt">
            <xs:attribute name="TriggerIdentifier" type="xs:string"
use="required"/>
            <xs:attribute name="TimeUnitMultiplier" type="xs:int"
use="required"/>
            <xs:attribute name="TriggerExecutionDate" type="xs:string"
use="required"/>
```

```
            <xs:attribute name="LifecycleStartDate" type="xs:string"
use="required"/>
      </xs:attributeGroup>
      <xs:element name="TriggerUserDefined" type="dis:TriggerUserDefined"/>
      <xs:complexType name="TriggerUserDefined">
            <xs:sequence>
                  <xs:element ref="add:AdditionalInformation"/>
                  <xs:any minOccurs="0" maxOccurs="unbounded"
processContents="lax"/>
            </xs:sequence>
            <xs:attributeGroup ref="dis:TriggerUserDefinedAtt"/>
      </xs:complexType>
      <xs:attributeGroup name="TriggerUserDefinedAtt">
            <xs:attribute name="TriggerIdentifier" type="xs:string"
use="required"/>
      </xs:attributeGroup>
      <xs:element name="Event" type="dis:Event"/>
      <xs:complexType name="Event">
            <xs:sequence>
                  <xs:element ref="dis:EventUserDefined"/>
            </xs:sequence>
            <xs:attributeGroup ref="dis:EventAtt"/>
      </xs:complexType>
      <xs:attributeGroup name="EventAtt">
            <xs:attribute name="EventIdentifier" type="xs:string"
use="required"/>
            <xs:attribute name="EventName" type="xs:string" use="required"/>
      </xs:attributeGroup>
      <xs:element name="EventUserDefined" type="dis:EventUserDefined"/>
      <xs:complexType name="EventUserDefined">
            <xs:sequence>
                  <xs:element ref="add:AdditionalInformation"/>
                  <xs:any minOccurs="0" maxOccurs="unbounded"
processContents="skip"/>
                  </xs:sequence>
            <xs:attributeGroup ref="dis:EventUserDefinedAtt"/>
      </xs:complexType>
      <xs:attributeGroup name="EventUserDefinedAtt">
            <xs:attribute name="EventIdentifier" type="xs:string"
use="required"/>
      </xs:attributeGroup>
</xs:schema>
```

Vital Records Review Schema

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:ns1="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/VitalRecordRev
iew"
xmlns:add="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/AdditionalInfo
rmation"
xmlns:ns2="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/Event"
targetNamespace="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/VitalRec
ordReview" elementFormDefault="qualified" >
<xs:import
namespace="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/Event"
schemaLocation="Event.xsd"/>
<xs:import
namespace="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/AdditionalInfo
rmation" schemaLocation="AdditionalInformation.xsd"/>

      <xs:element name="VitalRecordReview" type="ns1:VitalRecordReview"/>
      <xs:complexType name="VitalRecordReview">
            <xs:sequence>
             <xs:element name="VitalRecordReviewType">
              <xs:complexType>
                        <xs:choice>
                           <xs:element name="Cutoff" type="xs:string"/>
                           <xs:element name="VitalRecordsReview"
type="xs:string"/>
                           <xs:element name="InterimTransfer"
type="xs:string"/>
                        </xs:choice>
                  </xs:complexType>
              </xs:element>
              <xs:element name="VitalRecordReviewMode">
                   <xs:complexType>
                        <xs:choice>
                              <xs:element name="Time" type="xs:string"/>
                        <xs:element name="Event" type="xs:string"/>
                        <xs:element name="TimeEvent" type="xs:string"/>
                         </xs:choice>
                        </xs:complexType>
                   </xs:element>
                   <xs:element name="TimeUnitType">
                        <xs:complexType>
                              <xs:choice>
                                    <xs:element name="Fiscal"
type="xs:string"/>
                                    <xs:element name="Calendar"
type="xs:string"/>
                         </xs:choice>
                         </xs:complexType>
                  </xs:element>
                  <xs:element name="Event">
                        <xs:complexType>
                         <xs:sequence>
                              <xs:element ref="ns1:Event"/>
                         </xs:sequence>
                  </xs:complexType>
              </xs:element>
                  <xs:element name="TimeUnit">
                   <xs:complexType>
                        <xs:choice>
                              <xs:element name="Daily" type="xs:string"/>
                              <xs:element name="Weekly" type="xs:string"/>
                              <xs:element name="Monthly" type="xs:string"/>
                              <xs:element name="Quarterly" type="xs:string"/>
                              <xs:element name="SemiAnnually"
type="xs:string"/>
                              <xs:element name="Annually" type="xs:string"/>
                           </xs:choice>
                        </xs:complexType>
                  </xs:element>
                  <xs:element ref="ns1:VitalRecordUserDefined"/>
                  </xs:sequence>
            <xs:attributeGroup ref="ns1:VitalRecordReviewAtt"/>
      </xs:complexType>
      <xs:attributeGroup name="VitalRecordReviewAtt">
            <xs:attribute name="VitalRecordReviewIdentifier" type="xs:string"
use="required"/>
            <xs:attribute name="TimeUnitMultiplier" type="xs:int"
use="required"/>
            <xs:attribute name="ViatlRecordReviewExecutionDate"
type="xs:string" use="required"/>
      </xs:attributeGroup>
      <xs:element name="VitalRecordUserDefined"
type="ns1:VitalRecordUserDefined"/>
      <xs:complexType name="VitalRecordUserDefined">
            <xs:sequence>
                  <xs:element ref="add:AdditionalInformation"/>
                  <xs:any minOccurs="0" maxOccurs="unbounded"
processContents="lax"/>
            </xs:sequence>
            <xs:attributeGroup ref="ns1:VitalRecordUserDefinedAtt"/>
      </xs:complexType>
      <xs:attributeGroup name="VitalRecordUserDefinedAtt">
            <xs:attribute name="VitalRecordReviewIdentifier"
type="xs:string"/>
      </xs:attributeGroup>
      <xs:element name="Event" type="ns1:Event"/>
      <xs:complexType name="Event">
            <xs:sequence>
```

```
                  <xs:element ref="ns1:EventUserDefined"/>
            </xs:sequence>
            <xs:attributeGroup ref="ns1:EventAtt"/>
       </xs:complexType>
      <xs:attributeGroup name="EventAtt">
            <xs:attribute name="EventIdentifier" type="xs:string" 
use="required"/>
            <xs:attribute name="EventName" type="xs:string" use="required"/>
      </xs:attributeGroup>
      <xs:element name="EventUserDefined" type="ns1:EventUserDefined"/>
      <xs:complexType name="EventUserDefined">
            <xs:sequence>
                  <xs:element ref="add:AdditionalInformation"/>
                  <xs:any minOccurs="0" maxOccurs="unbounded" 
processContents="skip"/>
                  </xs:sequence>
            <xs:attributeGroup ref="ns1:EventUserDefinedAtt"/>
      </xs:complexType>
      <xs:attributeGroup name="EventUserDefinedAtt">
            <xs:attribute name="EventIdentifier" type="xs:string" 
use="required"/>
      </xs:attributeGroup>
</xs:schema>
```

Lifecycle Phase Schema

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:add="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/AdditionalInfo
rmation"
xmlns:ns1="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/LifecyclePhase
"
targetNamespace="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/Lifecycl
ePhase" elementFormDefault="qualified">
      <xs:import
namespace="urn:http://jitc.fhu.disa.mil/recmgt/transferschemas/AdditionalInfo
rmation" schemaLocation="AdditionalInformation.xsd"/>
      <xs:element name="LifecyclePhase" type="ns1:LifecyclePhase"/>
      <xs:complexType name="LifecyclePhase">
            <xs:sequence>
                  <xs:element ref="ns1:LifeCyclePhaseUserDefined"/>
            </xs:sequence>
            <xs:attributeGroup ref="ns1:LifecyclePhaseAtt"/>
      </xs:complexType>
      <xs:attributeGroup name="LifecyclePhaseAtt">
            <xs:attribute name="LifecyclePhaseIdentifier" type="xs:string"
use="required"/>
            <xs:attribute name="LifeCyclePhaseName" type="xs:string"
use="required"/>
            <xs:attribute name="LifecyclePhasePrecedence" type="xs:int"
use="required"/>
      </xs:attributeGroup>
      <xs:element name="LifeCyclePhaseUserDefined"/>
      <xs:complexType name="LifeCyclePhaseUserDefined" >
            <xs:sequence>
                  <xs:element ref="add:AdditionalInformation"/>
                  <xs:any minOccurs="0" maxOccurs="unbounded"
processContents="lax"/>
            </xs:sequence>
            <xs:attributeGroup ref="ns1:LifeCyclePhaseUserDefinedAtt"/>
      </xs:complexType>
      <xs:attributeGroup name="LifeCyclePhaseUserDefinedAtt">
            <xs:attribute name="LifecyclePhaseIdentifier" type="xs:string"
use="required"/>
      </xs:attributeGroup>
</xs:schema>
```